IT-ADMINISTRATOR.DE

02/2011

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Sicherheit von Unternehmensdaten

4 196583 126051 02

www.lancom.de/wlan

. . . connecting your business

Made in Germany

WLAN mit Hochverfügbarkeitsgarantie? Von LANCOM!

Mit der LANCOM Smart Controller-Architektur sorgen wir für maximale Ausfallsicherheit im WLAN: was immer passiert, das Funknetz steht weiter zur Verfügung.

Davon profitieren kleine WLANs genauso wie Netze mit Tausenden von Access Points, der Hotspot genauso wie die Installation im Freien. Und: Wireless LANs von LANCOM skalieren perfekt – so wächst Ihr Netz ganz einfach mit Ihren Bedürfnissen.

Setzen auch Sie auf WLAN von der deutschen Nummer EINS! Exzellenter Service, kostenlose Updates & Investitionsschutz inklusive.

CeBIT Halle 13 Stand C28

LANCOM Systems

EDITORIAL

Sicherheit – mehr als nur ein Bonus

Liebe Leser,

sie verfügen über Fertigkeiten, von denen so manche Programmierer nur träumen können: Hacker – Fluch und Segen für die IT-Welt. Während White-Hats Schwachstellen aufdecken und den Herstellern melden, um Schlimmeres zu verhindern, nutzen Black-Hats alles an Lücken aus, was sie in die Finger bekommen. Dabei machen es ihnen die Software-Hersteller oft mit eilig zusammengeschusterten Programmcodes allzu leicht. Die IT-Nutzer haben das Nachsehen und bleiben sich selbst überlassen. Unzählige Applikationen sind fortwährend zu patchen, neue Versionen einzuspielen, komplexe Einstellungen richtig zu setzen. Eine Arbeit, die selbst erfahrene IT-User überfordert – zumindest zeitlich. Zudem tun sich Administratoren oft schwer, laufend Updates in Produktivumgebungen einzuspielen. Zu groß ist das Risiko, wichtige Server ungewollt lahmzulegen.

Höchste Zeit also, Sicherheit von Grund auf neu zu überdenken und neben dem Sicherheitsrisiko Anwender zumindest die Gefahr durch löchrige Software aus der Welt zu schaffen. Softwarehersteller müssen verstehen, dass ihre Produkte essenzieller denn je für Wirtschaft und Gesellschaft sind. Diese sicherheitstechnisch bei den Kunden reifen zu lassen, ist nicht angemessen – und war es noch nie. IT-Systeme müssen vielmehr von Anfang an mit Blick auf ihre Sicherheit entworfen und nicht bereits dann auf die Allgemeinheit losgelassen werden, wenn keine offensichtlichen Fehler mehr auftauchen. Zahlreiche Hersteller haben zwar in den letzten Jahren ihre Qualitätskontrollen ausgebaut. Doch viel an der grundlegenden Problematik geändert hat dies nicht. Natürlich müssen dabei zwei Dinge klar sein: Sicherheit kostet immer Geld und absolute Sicherheit kann es nie geben.

Solange wir also noch auf Produkte hoffen dürfen, die verlässlich arbeiten und vertretbar sicher sind, haben Antivirus-Suiten alle Hände voll zu tun, unsere Rechner zu schützen. Sechs solcher Suiten für kleine und mittlere Umgebungen nehmen wir in unserem großen Vergleichstest ab Seite 16 mit Hilfe der Spezialisten von AV-Test genau unter die Lupe. Dabei müssen die Virenjäger zeigen, wie effektiv sie Malware abwehren und wie praxistauglich sie im IT-Alltag sind. Zudem beweist die Software "Lumension Patch and Remediation 7.0", wie effektiv sie Admins bei der lästigen Patchverteilung unterstützt.

Viel Spaß beim Lesen, Ihr

Daniel Richey
Stellv. Chefredakteur

notebooksbilliger.de Business

DELL PowerEdge T110 Server

www.notebooksbilliger.de/dellserver

- max. 4 x 3,5" HDD
- bis zu 16 GB RAM
- innerhalb 24h lieferbar
- inklusive 1–3 Jahre Vor-Ort-Service-Garantie

ab 329 €*

DELL™

Für Ihr individuelles Angebot
erreichen Sie unser Consultingteam unter

0331 73099 034

* Preis exkl. Mehrwertsteuer und zzgl. Versandkosten. Angebot gilt für ausgewählte Systeme solange der Vorrat reicht. Irrtümer, Druck- und Schreibfehler sind vorbehalten.

INHALT

IT-Administrator – Ausgabe Februar 2011

Sicherheit von Unternehmensdaten

Einkaufsführer: Hybrides Backup lokal und in der Cloud

Neben lokal implementierten Disaster-Recovery-Lösungen für physikalische und virtuelle Umgebungen rücken zunehmend Services für die Image-basierte Sicherung in der Cloud ins Blickfeld, die vor allem für kleine und mittlere Unternehmen mit begrenzten IT-Budgets attraktiv werden. Dabei gilt es, sowohl für die Implementierung einer Online-Backup-Lösung als auch auf der lokalen Seite wichtige Punkte zu beachten, damit die drei Ebenen aus physikalischem, virtuellem und Cloud-Backup harmonieren und sich ergänzen. Dieser Einkaufsführer erläutert, was beim Einkauf von Backupkapazitäten in der Cloud zu beachten ist und welche lokalen Voraussetzungen zu schaffen sind.

Seite 35

Bladeserver-Management mit HP Virtual Connect (1)

In unserem Einkaufsführer im Januar haben wir Ihnen aufgezeigt, welche technischen Möglichkeiten Sie sich mit dem Einsatz der Bladeserver-Technologie ins Rechenzentrum holen. Doch birgt diese Technik auch Fallstricke. In unserer zweiteiligen Workshopserie zeigen wir Ihnen auf, wie Sie ein solches System verwalten und welche erweiterten Optionen Ihnen hierfür der HP Virtual Connect Enterprise Manager bietet.

Seite 62

Neu im IT-Administrator: Link-Codes

Unsere neuen Link-Codes ersparen Ihnen mühsame Tipparbeit bei langen URLs

Skalierbares NAS für KMUs

Mit der **DS1511+** präsentiert **Synology** einen skalierbaren zentralen **NAS-Speicher** für den Einsatz in Unternehmen kleiner bis mittlerer Größe. Durch den Einsatz von bis zu zwei **DX510-Erweiterungsstations** lässt sich diese ursprünglich fünf Festplatteneinschübe umfassende DiskStation auf bis zu 15 Festplatten und eine maximale Speicherkapazität von 45 TByte aufrüsten. Zudem bietet das Betriebssystem DiskStation Manager 3.0 unternehmensrelevante Anwendungen zum Hosten von Websites oder einfachen Verwalten der Zugangsberechtigungen. Der Standard-Arbeitsspeicher von 1 GByte lässt sich auf 3 GByte aufrüsten, um die Leistungsfähigkeit zu erhöhen. Ausgestattet mit einem 1,8 GHz Dual-Core Prozessor verbraucht die DS1511+ 68 Watt Strom im laufenden Betrieb. Der Energiekonsum wird durch programmiertes Ein- und Ausschalten, den Festplatten-Ruhemodus und die Wake on LAN/WAN-Funktion zusätzlich reduziert. Die Station besitzt zwei LAN-Ports und Hot-Swap Festplatteneinschübe, um eine ausfallsichere Verfügbarkeit der Daten zu gewährleisten. Die Synology Disk-

Die DS1511+ von Synology lässt sich auf bis zu 45 TByte aufrüsten

Station DS1511+ ist ab sofort zu einem Preis von 635 Euro, die Erweiterungsstation DX510 für 380 Euro erhältlich. *(dr)*

Synology: www.synology.com/deu/products/DS1511+/

Überarbeitete Thin Client-Suite für lau

openthinclient bringt seine **openthinclient Software-Suite** in **Version 1.0** auf den Markt. Durch ein umfassendes **Kernel- und Systemupdate** stellen die Entwickler neben vielen anderen Neuerungen die Unterstützung aktueller Hardware sowie die Möglichkeit zur Anbindung von Zweigstellen mit geringer Bandbreite und ohne eigene Serverinfrastruktur zur Verfügung. Zusätzlich zum üblichen Netzwerkboot via PXE bietet die Software-Suite ab Version 1.0 die Option eines lokalen Systemstarts (Localboot) mit zentralen Konfigurations- und Update-Möglichkeiten. Dies erlaubt nun zusätzlich einen serverunabhängigen Startvorgang. Durch ein umfangreiches Kernel- und Treiberupdate im 1.0-Release können aktuelle Atom- und ION-basierte Thin Clients mit zahlreichen Peripheriegeräten betrieben werden. Darüber hinaus wurde eine Smart-Card-Unterstützung via RDP und ICA integriert. Auch den openthinclient-Manager haben die Entwickler für das 1.0-Release um wesentliche Eigenschaften erweitert. So ist er jetzt mandantenfähig, erlaubt also eine Entlastung der Administratoren, indem berechtigte Help-Desk-Mitarbeiter Informationen im Management-Interface einsehen können. Der openthinclient-Manager 1.0 ermöglicht darüber hinaus den Import und Export aller Konfigurationsdaten sowie die Duplikation von Konfigurationsobjekten. Eine ganze Reihe weiterer Neuerungen und Verbesserungen rundet das 1.0-Release ab. So stehen neben vielen anderen nun die aktuellsten Versionen von Citrix Receiver 11, Firefox 3.6, Thunderbird 3.1 und Open Office 3.2 als Installationspakete bereit. Die Software-Suite 1.0 steht zum kostenfreien Download auf der Herstellerseite zur Verfügung. *(dr)*

openthinclient: http://openthinclient.org

Kleiner Leistungsträger

CONCEPT International erweitert sein Portfolio um einen leistungsstarken **Mini-PC** mit NVIDIAs hochperformanten GeForce ION-Grafikchip und Intels 2,5 GHz Core 2 Duo-CPU. Der **miniPC 325i** besitzt zwei digitale Monitoranschlüsse (DVI/HDMI) und erlaubt die simultane und ruckelfreie Darstellung von unterschiedlichen Full-HD-Inhalten auf zwei Bildschirmen. Der Rechner arbeitet dank der Verwendung von FlashROMs oder SSDs ohne bewegliche Teile, wodurch ein wartungsfreier und langlebiger Betrieb möglich sein soll. Weitere technische Merkmale sind unter anderem vier USB 2.0-Ports sowie ein serieller Anschluss. Zur Kommunikation in Netzwerken steht neben einem GBit-Ethernet-Anschluss, der ein unterbrechungsfreies HD Video-Streaming erlaubt, optional zur kabellosen Kommunikation ein 802.11n WLAN- oder UMTS-Modul zur Verfügung. Dabei bleibt der miniPC 325i mit seinen kompakten Abmessungen (14,8 x 16,5 x 5,5 cm) etwa so groß wie drei aufeinanderliegende DVD-Hüllen. Als Betriebssysteme stehen Windows XP Professional, Windows embedded und Windows 7 zur Auswahl.

Der CONCEPT miniPC 325i setzt auf SSDs und FlashROMs für einen verlässlicheren Betrieb

Preislich bewegt sich der Rechner je nach Ausstattung zwischen 900 und 1.000 Euro. *(dr)*

CONCEPT: www.concept.biz

Grafikwandler für unterwegs

LINDY stellt einen **3in1-Adapter** für die Konvertierung des **Mini DP-Signals** in **HDMI**, **DVI** oder **Standard-DP** vor. Technisch wird das DP-Signal mit Hilfe eines integrierten Chips aktiv in DVI oder HDMI umgerechnet. Der hier verwendete Chip benötigt keine zusätzliche Stromversorgung und liefert eine Full HD-Auflösung für HDMI mit 1.080 Pixeln und 1.920 x 1.200 für DVI. Für eine direkte Umwandlung von Mini DP auf den normalen DisplayPort kann bei einer Farbtiefe von 36/12 Bit eine Auflösung von 2.560 x 1.600 übertragen werden. Für diese Auflösungen unterstützt der Adapter TMDS und steht zudem in Einklang mit den VESA Interop Guidelines. Im kompakten Gehäuse verbindet der Adapter Anschlüsse sowohl für große DisplayPort-, DVI- als auch HDMI-Anschlusskabel. So können Nutzer auch unterwegs ihren Computer an ein vorhandenes TV-Gerät, einen Monitor oder Projektor anschließen. Für rund 25 Euro ist der Adapter erhältlich. *(dr)*

LINDY: www.lindy.de

Der kompakte LINDY 3in1-Adapter wandelt das Mini DP-Signal in HDMI, DVI und Standard-DP um

Vier neue Funker im Netgear-Portfolio

Netgear präsentiert vier neue **Wireless-Router**. Zu den neuen Produkten zählen die beiden **Dualband Gigabit Router N600** (WNDR3800) und **N750** (WNDR4000), das **All-In-One-Gateway N600** (DGND3700) mit integriertem Modem sowie ein **N300-Wireless Router** mit kombiniertem **Powerline AV** (WNXR2000). Der "N600 Wireless Dualband Gigabit Router" überträgt auf 2,4 GHz und 5 GHz brutto jeweils 300 MBit/s. Dabei bietet das Gerät Funktionen wie "ReadyShare Remote" für den Zugriff auf Dateien und Ordner von jedem Mac, PC oder mit dem Internet verbundenen Smartphones und Tablets auf externe USB-Speichergeräte, die mit dem Router verbunden sind. "ReadyShare Printer" bindet zudem USB-Multifunktionsdrucker in das Netzwerk ein und ermöglicht drahtloses Drucken. Das Feature "Clear Channel Selector" soll außerdem für schnelle und störungsfreie Wireless Verbindungen sorgen und die Nutzung hoch beanspruchter WLAN-Kanäle automatisch und dynamisch vermeiden. Das Gateway "N600 Wireless Dualband Gigabit ADSL Modemrouter" kombiniert zudem ein integriertes ADSL-Modem mit einem Wireless Router und GBit-Ethernet. Anwender können so verschiedene Breitband-Technologien mit einem einzigen Gerät nutzen. Der Netzstecker des Powerline-Modells N300 integriert 200 MBit/s Powerline und macht das hauseigene Stromnetz somit bereit für eine Vernetzung per Powerline. Die neuen Modelle WNDR3800, WNDR4000 sowie DGND3700 sollen im Verlauf des zweiten Quartals 2011 verfügbar sein. Die Preise will der Hersteller mit der jeweiligen Produktverfügbarkeit bekanntgeben. Die Powerline-Variante WNXR2000 ist für rund 75 Euro erhältlich. *(dr)*

Das Gateway N600 von Netgear bietet eine WLAN-Schnittstelle sowie ADSL-Internetzugang

Netgear: www.netgear.com

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

Greenbone Networks bietet mit dem **Greenbone Security Explorer** ein browserbasiertes Plug-In an, das die aktuelle Sicherheitslage im Unternehmensnetzwerk auf einer Weltkarte darstellt. Über den Mauszeiger steuern Administratoren die einzelnen Standorte an, um Informationen zur Bedrohungslage abzurufen und notwendige Gegenmaßnahmen zu ergreifen. Dafür sammelt das Werkzeug über ein entsprechendes Berichtsformat sicherheitsrelevante Informationen zu weltweit durchgeführten Schwachstellen-Scans. Das Plug-In verbildlicht die Ergebnisse dann wahlweise mit Hilfe von Google Maps oder OpenStreetMap als Hintergrundkarte. Das Tool ist Teil des Greenbone Security Managers 1.4, der zu einem Preis ab 9.200 Euro erhältlich ist. *(ln)*

www.greenbone.net

Panda Security bietet **Version 5.05 von Panda Cloud Office Protection** an. Das Hauptmerkmal der neuen Version ist eine vereinfachte Verwaltung, dank derer individuelle Einstellungen nicht mehr zwingend von Grund auf neu angelegt werden müssen. Ermöglicht wird diese Vereinfachung durch die Funktion, Profile der Client-Datenbanken mit einem Klick zu kopieren, zu verändern und zu teilen. Die neue Panda Cloud Office Protection beinhaltet zudem eine noch leistungsstärkere Erkennungs-Engine. Ab 2.000 Euro für 50 Lizenzen ist die Antiviren-Lösung verfügbar. *(dr)*

http://cloudprotection.pandasecurity.com

Zertificon stellt das **Z1 SecureMail Gateway 4.3** bereit. Es verschlüsselt und signiert den E-Mailverkehr und ist in seiner aktuell erschienenen Version noch flexibler einsetzbar. So wurde unter anderem das Mandantenmodell erweitert: Ab sofort können die User mit gleicher Maildomäne auf unterschiedliche Z1 SecureMail Gateway-Mandante verteilt werden. Auch die Performance hinsichtlich der Verarbeitung von Nachrichten mit hohen Datenmengen sowie die Admin-GUI will der Hersteller verbessert haben. Für 20 aktive Clients kostet das Gateway 1.330 Euro. *(dr)*

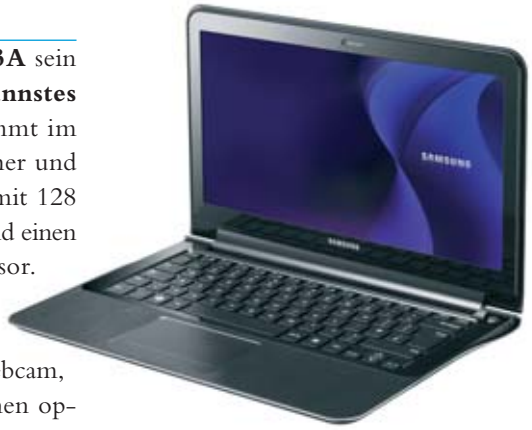
www.zertificon.com

Kerio Technologies stellt mit **Kerio Operator** eine neue IP-PBX-Lösung für kleine und mittelständische Unternehmen vor. KerioOperator basiert auf der Open-Source-Software Asterisk und nutzt zur Anbindung von Endgeräten das VoIP-Standardprotokoll SIP. Verbindungen zum öffentlichen Telefonnetz stellt Kerio Operator über SIP-Trunks, T1/E1- oder Euro-ISDN-Anschlüsse her. Die IP-PBX ist als Software-Appliance mit einem eigenen gehärteten Betriebssystem sowie als virtuelle Appliance für VMware und Hardware-Appliance namens Kerio Operator Box erhältlich. Die Preise für Kerio Operator beginnen bei 480 Euro. *(dr)*

www.kerio.de

Schlanker Reisebegleiter

Samsung stellt mit dem **900X3A** sein mit maximal 16 mm bislang **dünnstes Notebook** vor. Das Gerät kommt im **13,3 Zoll-Format** (34 cm) daher und beinhaltet eine SSD-Festplatte mit 128 GByte, 4 GByte Arbeitsspeicher und einen Intel Core i5 2520 UM-Prozessor. Die Akkulaufzeit soll bis zu sieben Stunden betragen. An Ausstattung bietet das Gerät eine Webcam, Bluetooth 3.0, USB 3.0 und einen optionalen externen DVD-Brenner. Das Innere des Rechners wird durch ein robustes und hochwertig verarbeitetes Duraluminium-Gehäuse geschützt. Die schnelle und komfortable FastStart-Funktion gewährt innerhalb weniger Sekunden Zugriff auf persönliche Daten sowie E-Mails, den Kalender oder das Internet. Für ungestörtes Arbeiten auch bei hellem Tageslicht wartet das SuperBright-LED-Display des Rechners mit einer Lichtstärke von 400 nit auf und ist im Vergleich zu gewöhnlichen Notebook-Displays (laut Samsung durchschnittlich rund 220 nit) um ein Vielfaches heller. Als Betriebssystem läuft auf dem Notebook Windows 7 Professional 64 Bit. Für rund 1.340 Euro ist der Rechner erhältlich. *(dr)*



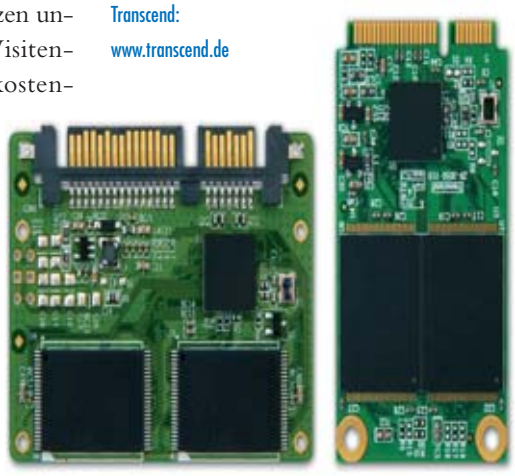
Das Notebook 900X3A von Samsung ist nur zwischen sechs und 16 mm dick

Samsung: www.samsung.de

Liebling, ich habe die SSDs geschrumpft

Transcend Information erweitert seine Produktpalette um Low-Profile mSATA-Karten und Half-Slim Solid State Drives (SSD). Diese **besonders kompakten Flash-Speicher** wurden vom Hersteller für Geräte konzipiert, die einen kleinen Formfaktor benötigen – wie etwa dünne und leichte Notebooks, Netbooks, Tablets oder GPS-Geräte. Beide neuen SSD-Speicherformate besitzen ungefähr die Abmessungen einer Visitenkarte und sind laut Transcend kostengünstiger als die meisten 2,5 Zoll-SSDs. Die SATA-Schnittstelle weist bei beiden Produktlinien eine Bandbreite von 3 GBit/s. auf. Die unter der Produktnummer MSA300 veröffentlichten mSATA-SSDs messen 29,85 x 50,8 x 3,5 mm und entsprechen dem JEDEC MO-300A-Standard. Sie sind in Kapazitäten von 32 und 64 GByte erhältlich und kosten 66 beziehungsweise 125 Euro. Die Half-Slim-SSDs mit der Bezeichnung SSD25H-M sind etwas größer (54 x 39 x 4 mm), jedoch immer noch kleiner als 2,5 Zoll-Modelle, verwenden aber den gleichen SATA-Connector wie 2,5 Zoll-Speichermedien. Die Half-Slim-SSDs sind konform mit dem Standard MO-297 JEDEC. Sie fassen zwischen 4 und 64 GByte und sind zu Preisen zwischen 21 und 125 Euro verfügbar. *(ln)*

Transcend:
www.transcend.de



Transcend bietet mit neuen Half-Slim-SSDs (links) und mSATA-Karten besonders kompakte Flash-Speicher an

Modularer Strom für 19-Zoll-Schränke

U.T.E. Electronic stellt die **USV-Baureihe AP160** vor, die aus **zwei Modulen** besteht und im Leistungsbereich von **1 bis 6 kVA** arbeitet. So versorgen die insgesamt vier USV-Modelle in der jeweils höchsten Ausbaustufe angeschlossene IT-Systeme zwischen 94 und 154 Minuten mit Strom. In Bezug auf den Formfaktor hat der Hersteller die Einbautiefe reduziert, wodurch sich die USV auch in kürzeren Schränken problemlos installieren lassen soll. Die USV-Anlage besteht aus zwei separat im Schrank zu installierenden Komponenten. Dies ist zum einen ein Steuermodul, das alle aktiven Komponenten wie Gleich-/Wechselrichter, Stromversorgungs- und Kommunikationsanschlüsse, LCD-Display sowie den Bypass beinhaltet. Das zweite Modul dient zur Aufnahme der Batterien und lässt sich über ein Kabel und Steckkontakt mit dem Steuermodul verbinden. Bei einem eventuellen Servicefall können so die Batterien im Schrank bleiben. Sogar eine notwendige, etwa durch zusätzliche Verbraucher verursachte Leistungserhöhung kann mit dem raschen Austausch des Steuermoduls erledigt werden. Da Batterien von USV-Anlagen einer Alterung unterliegen, kann es vorkommen, dass diese nach einigen Jahren gewechselt werden müssen. Hier bietet das Modul den Vorteil, dass alle Anschlussleitungen der USV im Schrank unberührt bleiben können, da nur Zugang zum Batteriemodul benötigt wird. Zudem reduziert die modulare Bauweise die Einbautiefe der USV-Anlage, was Vorteile bei weniger tiefen 19-Zoll-Schränken mit sich bringt. Die verwendete Dauerwandlertechnik schützt zudem nicht nur gegen Stromausfall, sondern gegen eine Vielzahl von Netzstörungen. Zur Kommunikation stehen SNMP-Adapter und potentialfreie Kontakte als Einsteckkarten optional zur Verfügung. Die Preise liegen zwischen 600 und 2.670 Euro. *(dr)*

U.T.E. Electronic: www.ute.de/usv/online/gtec-ap160/

Thin Client meistert vier Monitore

Mit dem Modell **E3505** stellt **Rangee** einen neuen **Thin Client mit Multimonitor-Support** vor. Das Gerät verfügt bereits in der Serienausstattung über zwei DVI-Ausgänge. Die digitalen Monitoranschlüsse erlauben Auflösungen von bis zu 1920 x 1440 Bildpunkten gleichzeitig auf beiden Bildschirmen. Neben dem serienmäßig möglichen Dualmonitorbetrieb ist der schlanke Rechner bereits auf den Anschluss eines dritten und eines vierten Bildschirms vorbereitet. Hierfür hat der Hersteller eine PCIe-Schnittstelle auf dem Mainboard implementiert, die den Einbau einer Grafikkarte mit ebenfalls zwei DVI-Ausgängen erlaubt. Die Basis der neuen Thin Clients stellt ein VIA-Eden-Prozessor mit einer Taktfrequenz von 1 GHz dar, dem 512 MByte DDR-2-RAM als Arbeitsspeicher zur Seite stehen. Peripherie lässt sich über sechs USB 2.0-Schnittstellen anschließen. Die Preise beginnen bei 257 Euro für das Modell E3505-PXE ohne Betriebssystem. Die Variante S-E3505-L verfügt über 256 MByte Flash-Speicher mit dem Rangee Linux-Betriebssystem und den Software-Modulen ICA, RDP, VMware View und Mozilla Firefox. Der Preis hierfür liegt bei 316 Euro. *(ln)*

Rangee: www.rangee.de

Zusätzlich zu den beiden ab Werk verbauten DVI-Anschlüssen lässt sich der Thin Client Rangee E3505 mit einer PCIe-Grafikkarte ausstatten

Gateway-Schutz 2.0

Blue Coat Systems stellt die neue **ProxyOne-Appliance** vor. Das Modell integriert einen **Filter für Webinhalte**, **Inline-Scanner für Malware und Viren** sowie detaillierte **Berichtsfunktionen**. Diese Kombination soll es mittelständischen Unternehmen ermöglichen, Web-2.0-Anwendungen sicherer zu nutzen. Dabei lässt sich die ProxyOne-Appliance auch von weniger spezialisierten IT-Generalisten in nur sechs Schritten installieren und konfigurieren. Zudem ist die Appliance mit vordefinierten Richtlinien ausgestattet und führt Softwareupgrades sowie Sicherheitsupdates automatisch durch. Das Modell nutzt den Blue Coat WebFilter und erhält über den Cloud-basierten Dienst Bewertungen von Webseiten in Echtzeit. Dabei erweitern die Sicherheitsexperten des Herstellers laufend die Abwehrfunktionen von WebPulse, um dessen Nutzer vor neuen Bedrohungen zu schützen. Durch die Inline-Prüfung des Datenverkehrs auf Malware und Viren am Webgateway blockiert ProxyOne ausführbare Malware, bevor diese in das Netzwerk gelangt. Durch Caching-Technologien beschleunigen die ProxyOne-Appliances den Scan-Prozess mit einem "Scan once, serve many"-Modell, so dass die Überprüfungen nicht auf Kosten der Performance gehen. Bis zu 100 MBit/s setzt das Gerät dabei durch. Um infizierte Benutzer zu identifizieren, stellt die Appliance zudem detaillierte Auswertungen webbasierter Benutzeraktivitäten bereit. Die ProxyOne-Appliance ist ab sofort verfügbar. Die Preise für das erste Jahr beginnen bei 8.999 Euro für 100 Benutzer. Darin enthalten sind die Appliance selbst sowie Softwarelizenzen, automatische Sicherheitsupdates und 24x7-Support. Insgesamt unterstützt die Appliance bis zu 2.000 Nutzer. *(dr)*

Blue Coat: www.bluecoat.de

Die ProxyOne von Blue Coat richtet sich durch ihre leichte Bedienung an kleine und mittelständische Unternehmen

Helpdesk-Mitarbeiter im Blick

helpLine veröffentlicht Version 5.1 seiner gleichnamigen ITIL V3-zertifizierten **Service-Management-Software**. Neu ist unter anderem die "Workforce Management" genannte Funktionalität, die eine Einsatzplanung auch für komplexe Aufgaben direkt in der Management-Lösung erlaubt. Das Modul beinhaltet etwa eine grafische Darstellung der Auslastung des Service-Teams bis hinunter zum einzelnen Service-Mitarbeiter. Auf Wunsch filtert helpLine dabei die Mitarbeiter nach Qualifikationsprofil und zeigt eine vollständige Übersicht der Auslastung inklusive geplanter Projektaufgaben, vorliegenden Service-Anfragen sowie Abwesenheiten an. Ebenfalls neu ist die zertifizierte Anbindung der Voice-over-IP-Lösung Microsoft Office Communication Server (OCS). Nutzer können via OCS direkt aus helpLine heraus telefonieren und erhalten beim Eingang eines Service-Anrufs alle hinterlegten Informationen in der Ticket-Maske. Weitere Verbesserungen der Benutzerfreundlichkeit umfassen laut Hersteller eine Online-Hilfe, Rechtschreibprüfung sowie eine Undo-Funktion für Texte und eine automatische Optimierung für das Arbeiten auf Citrix und Windows Terminal Servern. Die neue Version ist ab sofort erhältlich und kostet in einem Quick Start-Paket inklusive Implementierung, Lizenzierung und Schulung der Mitarbeiter rund 12.000 Euro. *(ln)*

helpLine: www.helpline.de

1&1 WEBHOSTING

„1&1 WebHosting bietet uns zahlreiche Inklusiv-Features, die unsere Homepage noch informativer und erfolgreicher machen. Für uns ist 1&1 der perfekte Partner."

Markus Fügenschuh
www.skischule-ostrachtal.de

IHRE PROFESSIONELLE HOMEPAGE

6 MONATE FÜR 0,– €/MONAT!*

MEMBER OF united internet

*Ausgewählte 1&1 Homepage-Pakete z.B. 1&1 Homepage Perfect 6 Monate für 0,– €/Monat, danach 6,99 €/Monat. Einmalige Einrichtungsgebühr 9,60 €. .info und .de Domain 0,29 €/Monat im ersten Jahr (danach .de Domain 0,49 €/Monat, .info Domain 1,99 €/Monat), keine Einrichtungsgebühr. 12 Monate Mindestvertragslaufzeit. Preise inkl. MwSt.

1&1 HOMEPAGE-PAKETE
6 MONATE FÜR 0,– €/Monat
danach ab 6,99 €/Monat*

ANGEBOT NUR GÜLTIG BIS 28.02.2011!

1&1, der größte Webhoster weltweit, garantiert beste Hosting-Qualität und wertvolle Inklusiv-Features:

Inklusiv-Domains!
Sichern Sie sich Ihre perfekte Internet-Adresse: Sie können aus den Domainendungen .de, .at, .info, .com, .net, .org, .biz oder.eu wählen.

Mehr Webspace!
Selbst für aufwändige Website-Projekte bieten Ihnen unsere Pakete ausreichend Webspace.

Webdesign-Software!
Adobe® Dreamweaver® CS4 und NetObjects Fusion® dienen als optimale Basis für hochwertiges Webdesign, sogar optimiert für die Ausgabe auf mobilen Endgeräten.

Entwickler-Tools
PHP6 (beta), Zend Framework, Versionsmanagement (git), Cron Jobs und Shell-Zugang bieten die perfekte Spielwiese für professionelle Webdesigner.

Grüne Rechenzentren!
Ihre Daten liegen sicher in unseren Hochleistungs-Rechenzentren, die mit Strom aus erneuerbaren Quellen betrieben werden. Das spart 30.000 Tonnen CO_2 pro Jahr.

z. B. 1&1 HOMEPAGE PERFECT

- 2 Inklusiv-Domains
- 4 GB Webspace
- UNLIMITED Traffic
- 5 MySQL-Datenbanken
- Zend Framework
- PHP6 (beta), PHP5
- Perl, Python
- SSI
- NetObjects Fusion® 1&1 Edition
- Google Sitemaps
- 24/7 Profi-Hotline
- uvm.

~~6,99 €/Monat*~~ **0,– €/Monat***
6 Monate 0,– €, danach nur 6,99 €/Monat.*

Weitere sensationelle Angebote, z. B. .de, .info Domains 1 Jahr für 0,29 €/Monat*, unter www.1und1.info.

1&1

Jetzt informieren und bestellen:
0 26 02 / 96 91
0800 / 100 668

www.1und1.info

IT-Administrator-Workshop "Netzoptimierung für Virtualisierung und Storage" am 10. März 2011 in Augsburg und am 7. April in St. Augustin

Netzoptimierung leicht gemacht

ITANet Workshop-Partner:

baramundi software AG

ITANet Workshop-Partner:

GIB Gesellschaft für Informationstechnik und -Beratung mbH

von John Pardey

Nur in einem soliden, gut geplanten Netzwerk bringen hochwertige Server und Storage-Komponenten auch ihre Bestleistung. Dabei verändern neue Technologien wie etwa Virtualisierung oder Voice over IP die Anforderungen an das Netzdesign. Unsere Workshops in Augsburg und St. Augustin führen Sie in dieses komplexe Thema ein, dessen Verständnis und Umsetzung modernen Netzwerken für Virtualisierung und Storage einen Leistungsschub beschert.

Die explosionsartige Verbreitung von virtuellen Maschinen in Rechenzentren führt zu erheblichen Managementproblemen an den Schnittstellen zwischen den physischen Servern und den Netzkomponenten (Switches). Die aktuellen Normentwürfe der IEEE führen daher Virtual Ethernet Port Aggregation (VEPA) ein. Dabei handelt es sich um eine Erweiterung des physischen und virtuellen Switching zur Reduzierung der Verwaltungskomplexität der vielen im Rechenzentrum eingesetzten Switching-Elemente. Erfahren Sie in unserem Workshop, wie VEPA das Management für die Server- und Netzadministratoren erleichtert und die Anzahl der zu verwaltenden Switching-Elemente und Element-Merkmale (Adresstabellen, Richtlinien für Sicherheits- und Service-Attribute und Konfigurationen) deutlich senkt.

Neue Standards für die Virtualisierung

Ebenfalls für jeden Virtualisierungs-Admin äußerst interessant ist der Standard IEEE 802.1Qbg, der das Edge Virtual Bridging definiert. Ein physikalischer Server kann dabei über mehrere virtuelle Server verfügen und den Zugriff auf diese Ressourcen über das angeschlossene Bridged LAN bereitstellen. Fester Bestandteil von VEPA ist der so genannte Inter-VM Hairpinning-Mechanismus: Bei virtuellen Rechnern müssen unter Umständen die Pakete an einen anderen virtuellen Rechner übermittelt werden. Sind beide virtuellen Rechner über den gleichen physikalischen beziehungsweise logischen Port zu erreichen, filtert der Eingangs-Port des angeschlossenen Switches diese Pakete aus und die Pakete werden nicht übermittelt.

Mit Hilfe des Hairpinning-Prozesses ist der Switch in der Lage, die betreffenden Pakete anschließend über den Empfangs/Ausgangs-Port zum virtuellen Zielrechner zurückzusenden. Unser Dozent und ausgewiesener Netzwerkexperte Mathias Hein legt Ihnen dar, wie dadurch das Management eines solchen Switch-Konstrukts erheblich vereinfacht wird und der externe Switch alle Kontrollfunktionen übernimmt.

Zusätzlich ist noch eine weitere Policy-Extension notwendig, um externe Switches in einer virtuellen Umgebung zu nutzen. Hier setzt 802.1Qbh an: Dieser Standard ermöglicht Edge Virtual Bridges die Replikation von Paketen über mehrere virtuelle Kanäle hinweg auf eine Gruppe von Remote-Ports. Dadurch lassen sich kaskadierte Ports für ein flexibles Netzdesign einrichten und die Bandbreite für Multicast, Broadcast-und Unicast-Frames effizient nutzen. Unser Workshop zeigt, wie Administratoren durch die in 802.1Qbh erweiterten Port-Funktionen Policys, ACLs, Filter, QoS

Ab sofort haben Sie bei unseren Workshops zu jedem Thema zwei Termine und vor allem Orte zur Auswahl. Einer der am häufigsten an uns in Sachen Workshops herangetragene Wunsch ist die Verkürzung der Anreise, denn viele unserer Leser konnten in der Vergangenheit trotz großem Interesse nicht immer an unseren Workshops teilnehmen. Zukünftig haben Sie die Wahl zwischen zwei Veranstaltungsorten, von denen zumindest einer in einer annehmbaren Zeit erreichbar sein sollte.

Kürzere Anreise für alle

und andere Parameter auf dem Switch frei festlegen können.

Mehr Geschwindigkeit im Storage-Netzwerk

Ein performantes Storage-Netzwerk ist das Herzstück der Server-Virtualisierung. Inzwischen haben sich auch im Storage-Bereich unterschiedliche Technologien etabliert und es konkurrieren Fibre Channel und der iSCSI um die Gunst der Anwender. In unserem Workshop gehen wir der Frage nach, welches der beiden Protokolle sich für welchen Einsatzzweck eignet und untersuchen zudem jeweils die Zukunftssicherheit.

Grundsätzlich liefert Fibre Channel niedrigere Verzögerungszeiten als iSCSI. Fibre Channel hingegen erfordert spezielle FC-Switches und kostspielige FC Host Based Adapter in jedem Server, während sich iSCSI dagegen auf standardmäßigen Gigabit-Ethernet-Komponenten realisieren lässt. Dozent Mathias Hein zeigt den Seminarteilnehmern auf, welche Konsequenzen dies auf Planung und Betrieb des SAN hat.

Zwei Termine zur Auswahl

Für alle IT-Verantwortlichen, die Virtualisierung und/oder ein SAN betreuen und verantworten, bietet unser Workshop sicher ein breites Spektrum neuer Erkenntnisse und Möglichkeiten. Neu ist ab 2011 auch, dass wir jeden Workshop an zwei Terminen anbieten (siehe auch Kasten "Kürzere Anreise für alle"). Die beiden inhaltlich identischen Workshops finden diesmal am 10. März in Augsburg und am 07. April in St. Augustin statt. So möchten wir sicherstellen, dass Sie mit geringem Zeit- und Kostenaufwand an unseren Workshops teilnehmen können. Dieses neue Format gilt ab sofort für alle unsere Workshops.

Alle Informationen zur Anmeldung und zum Workshop finden Sie im Kasten "Workshop Netzoptimierung für Virtualisierung und Storage". Die Anmeldung ist jeweils bis eine Woche vor dem Workshop-Termin möglich. Wir würden uns freuen, Sie begrüßen zu dürfen.

iLNet
Die System und Netzwerk User Group

Die Agenda des Workshops

10.00 Uhr: Begrüßung

10.15 Uhr: Switching und Virtualisierung Teil 1
- Switching mit TRILL: höhere Bandbreite bei niedrigeren Latenzzeiten
- Virtual Ethernet Port Aggregation (VEPA): vereinfachtes Switching für Server-Netze
- Inter-VM Hairpinning: effektives Switching für virtualisierte Server

Dozent: Mathias Hein

12:00 Uhr: Partnervortrag: Client-Lifecycle-Management: Automatisiert zu Windows 7 wechseln
- Vorbereitungen, Aufgaben und Herausforderungen vor dem Betriebssystemwechsel
- Risiken vermeiden mit dem Windows 7-Kompatibilitätscheck
- Windows 7 automatisiert installieren
- Beispielhaftes Migrationsszenario

Dozent: Gerd Conrad, baramundi AG

12:45 Uhr: Mittagspause

14:00 Uhr: Switching und Virtualisierung Teil 2

Dozent: Mathias Hein

15:00 Uhr: Partnervortrag: Weltweite Client-Lifecycle-Unterstützung
- Client-Lifecycle-Management weltweit
- Vorbereitung zum Rollout mit Windows 7
- PXE baramundi Server auf XEN Client unter SLES

Dozent: Michael Terkatz, GIb-mbH

15:45 Uhr: Pause

16:00 Uhr: Mehr Geschwindigkeit im Storage-Netz:
- Fibre Channel vs. iSCSI vs. Fibre Channel over IP: Einsatzziele und Problemfelder
- Was wird sich langfristig durchsetzen und warum?

Dozent: Mathias Hein

Ort

10. März 2011, Augsburg: Baramundi Software AG, Beim Glaspalast 1, 86153 Augsburg

7. April 2011, St. Augustin: Konrad-Adenauer-Stiftung e.V., Rathausallee 12, 53757 St. Augustin

Teilnahmegebühren

Für IT-Administrator-Abonnenten kostenlos. Haben Sie ein Abonnement des IT-Administrator und möchten einen Kollegen mitbringen, erheben wir für den zweiten Teilnehmer eine Schutzgebühr von 75 Euro (zzgl. 19 Prozent MwSt.). Verfügt Ihr Unternehmen über kein Abonnement, wird eine Schutzgebühr von 145 Euro (zzgl. 19 Prozent MwSt.) fällig.

Anmeldung bis zum 3. März (Augsburg) oder 31. März (Sankt Augustin) unter
www.it-administrator.de/workshops/

Workshop Netzoptimierung für Virtualisierung und Storage

IT-Administrator Exchange-Training am 14. April in Hamburg und 24. Mai in München

Exchange meistern

von John Pardey

Die Komplexität einer Exchange-Infrastruktur ist äußerst hoch und nur mit solidem Wissen ist der Administrator in der Lage, diese zuverlässig und verfügbar zu betreiben sowie wichtige Features bereitzustellen, die die Anwender für ihre tägliche Arbeit benötigen. Daher bietet IT-Administrator ein ganztägiges Exchange-Training in Hamburg und München an, das praxisnahes Know-how zu Hochverfügbarkeit, der Veröffentlichung von Exchange im Internet und Troubleshooting vermittelt.

Grundlage jeder Exchange-Infrastruktur ist die Verfügbarkeit der Server. So steigt dann auch unser Exchange-Training mit diesem Themenblock in den Seminartag ein. Hierbei legen wir ein besonderes Augenmerk auf die neuen Hochverfügbarkeitsfeatures unter Exchange 2010. Nach einem Blick auf das neue Design der Hochverfügbarkeit erfahren Teilnehmer, wie sie dies in der Praxis konfigurieren und verwalten.

Zugriff über das Internet und Troubleshooting

Ist so eine stabile Infrastruktur sichergestellt, wendet sich unser Training einer der aufwändigsten Administrationsaufgaben unter Exchange zu – der Veröffentlichung im Internet. Auf der Basis einer sicheren Bereitstellung und Veröffentlichung mit dem Microsoft Threat Management Gateway, dessen Konfiguration wir ausführlich besprechen, lassen sich nun Outlook Web Access, Outlook Anywhere und ActiveSync einrichten. Dabei kümmern wir uns um das Vorgehen für die Exchange-Versionen 2003, 2007 und 2010.

Der abschließende Teil des Trainings versorgt die Teilnehmer dann mit dem notwendigen Rüstzeug für den Fall, dass Exchange einmal Probleme bereitet. Unser Dozent Jürgen Haßlauer stellt die wichtigsten Tools für das Troubleshooting vor und zeigt, wie sich damit Probleme identifizieren und lösen lassen. Abgerundet wird der intensive Tag dann durch einen Blick auf Wege, die Leistung des Exchange-Servers zu überwachen und so proaktiv Probleme zu vermeiden.

So erfahren die Teilnehmer, welche Bereiche des Microsoft Exchange Servers unbedingt auf ihre Performance hin beobachtet werden müssen, um die Stabilität des Systems sicherzustellen.

Kleiner Kreis und kleiner Preis

Die Teilnehmerzahl des Trainings ist für beide Termine streng begrenzt, um eine optimale Wissensvermittlung sicherzustellen. Die maximal 25 Teilnehmer haben somit genug Zeit für Fragen und Diskussionen mit unserem Exchange-Experten Jürgen Haßlauer. Dieser vermittelt die Inhalte des Trainings anhand einer Präsentation und durch Live-Demos an einem Exchange-Testsystem. Die Teilnahmegebühr für Abonnenten des IT-Administrator beträgt dabei gerade einmal 95 Euro (zzgl. MwSt.).

Alle Informationen zur Anmeldung und zum Training finden Sie im Kasten "Exchange-Training 2011". Die Anmeldung ist jeweils bis eine Woche vor dem Termin möglich. Wir würden uns freuen, Sie begrüßen zu dürfen.

Die Inhalte des Trainings

Hochverfügbarkeit in Exchange Server 2010
- Design
- Konfiguration und Management

Veröffentlichung von Exchange (2003, 2007, 2010) ins Internet über TMG
- OWA
- Outlook Anywhere
- ActiveSync

Troubleshooting Exchange (2003, 2007, 2010)
- Einführung in Tools zur Fehlerdiagnose
- Performance Monitoring

Dozent: Jürgen Haßlauer, infoWAN

Die Trainings beginnen jeweils um 10 Uhr und enden gegen 17:30 Uhr.

Ort

14. April 2011, Hamburg: ExperTeach Training Center, Esplanade 6, 20354 Hamburg

24. Mai 2011, München: ExperTeach Training Center, Wredestr. 11, 80335 München

Teilnahmegebühren

Für IT-Administrator-Abonnenten 95 Euro (zzgl. MwSt.), ansonsten 165 Euro (zzgl. MwSt.). Der Preis beinhaltet die Seminarunterlagen, Verpflegung im Seminar sowie ein Mittagessen.

Anmeldung bis zum 7. April (Hamburg) beziehungsweise 17. Mai (München). Die Veranstaltung ist auf 25 Teilnehmer begrenzt. Anmeldung unter www.it-administrator.de/workshops

Exchange-Training 2011

Intelligente Technologien für einen smarten Planeten

Was bedeuten 1,3 Millionen Transaktionen pro Sekunde für dieses Auto?

Sie bedeuten, dass man den möglichen Käufer für dieses Auto ziemlich genau beschreiben kann. Acxiom, einer der weltweit führenden Anbieter von Marketing-Dienstleistungen und -Technologie, arbeitet mit IBM zusammen, um für Unternehmen aus über 7.000 Datenbanken detaillierte Informationen über die Wünsche ihrer Kunden zu gewinnen. Damit unterstützt Acxiom neun der zehn größten Autohersteller sowie Unternehmen aus allen wichtigen Industriezweigen. Die Grundlage dafür liefert IBM System x® mit Intel® Xeon® Prozessor. Damit kann Acxiom 9.360 unterschiedliche Systeme auf nur 264 eX5 Systeme konsolidieren – und zwar ohne Leistungseinbußen. Ein smartes Unternehmen braucht intelligente Software, Systeme und Services.

Machen wir den Planeten ein bisschen smarter. **ibm.com**/car/de

IBM®

Hier werden Daten sichtbar gemacht, die die Vorlieben verschiedener Personengruppen für bestimmte Automobiltypen zeigen.

intel Xeon® inside™

Leistungsstark. Intelligent.

Im Vergleichstest: Sechs Antivirus-Suiten

Wettstreit der Schädlingsbekämpfer

von Thomas Bär und Hendrik Pilz

Quelle: Ioannis Kounadeas - Fotolia.com

Ohne einen Virenschutz kommt kein Unternehmen aus – angesichts der geschätzten 40 Millionen digitaler Schädlinge. Zu groß ist das Risiko, das von bösartigen Programmen ausgeht. Während Antiviren-Lösungen für den heimischen Privat-PC mit vielen Zusatzfunktionen wie einer verbesserten Firewall oder einem Anti-Spam-Filter aufgewertet werden, sind solche All-in-one-Suiten im Unternehmensumfeld nicht immer erwünscht. Hier zählen andere Werte, allen voran die zentrale Administrierbarkeit. In unserem Vergleichstest betrachten wir sechs professionelle Antiviren-Lösungen.

Für Antiviren-Software im Unternehmensumfeld bedarf es hauptsächlich einer zentralen Management-Lösung, die möglichst automatisiert die AV-Signaturen und Programmaktualisierungen an die Client-Systeme verteilt. Weiter findet sich auf der Wunschliste der Administratoren die zentrale Übersicht über alle Client- und Serversysteme. Für unseren Test haben wir daher die nach einer Marktanalyse [1] des IT-Dienstleisters OPSWAT sechs gebräuchlichsten Antivirus-Suiten unter die Lupe genommen, die sich an KMUs richten und die nötigen Administrationsfunktionen bieten: AVG Internet Security Business Edition 2011, Avira AntiVir Professional, ESET Smart Security 4 Business Edition, G Data AntiVirus Enterprise 10, Kaspersky Anti-Virus 6.0 für Windows Workstation und McAfee Total Protection for Endpoint.

In Bezug auf die Management-Funktionen installierten wir die AV-Lösungen auf einem aktuellen Windows Server 2008 R2 in der x64-Ausprägung. Nach der Installation wurde die AV-Client-Software auf einen Windows XP x86- und Windows 7 x64-Client verteilt. Die Management-Software musste Client-Computer, die in einer Windows-AD-Domäne verwaltet werden, direkt auffinden können. Ein zweiter Test besteht darin, einen Windows XP-Rechner außerhalb der Domänenstruktur mit einem AV-Client per "Push"-Kommando auszustatten. Allen Lösungen ist die verschlüsselte Kommunikation zwischen Management-Konsole und den Clients gemein.

Mehrstufiges Testverfahren

Das Testverfahren für die Erkennung und Performance-Messung führte das Magdeburger Institut AV-Test [2] durch. Alle Tests wurden auf einem typischen Rechner unter Windows XP Professional 32 Bit in vier Rubriken durchgeführt. Die erste Rubrik namens "Webseiten-Attacken" simuliert den direkten Zugriff auf 13 infizierte Webseiten. Diese Webseiten sind zwar nicht unbedingt repräsentativ im statistischen Sinne, jedoch sehr typisch für Gefährdungen, der sich ein Internet-Surfer im Unternehmen im "Vorbeiklicken" aussetzt. Das Blockieren der Schädlinge auf diesen Seiten trennte im Test die Spreu vom Weizen – in keiner anderen Rubrik waren die Unterschiede in der Leistungsfähigkeit größer.

Die zweite Testrubrik bestand aus mehr als 200.000 aktuellen Viren, Würmern und Trojanern aus den verschiedenen Gattungen. Dieser als "Zoo Malware-Erkennung" bezeichnete Test zeigt, wie effektiv die Programmierer einer AV-Software ihre Lösung auf den Praxiseinsatz trimmen konnten. Da es auch in dieser Kategorie zu nennenswerten Unterschieden kam, sei darauf hingewiesen, dass jede AV-Lösung in ihrer vom Hersteller gewählten Standardeinstellung ans Werk ging. Verfügt die AV-Lösung bei-

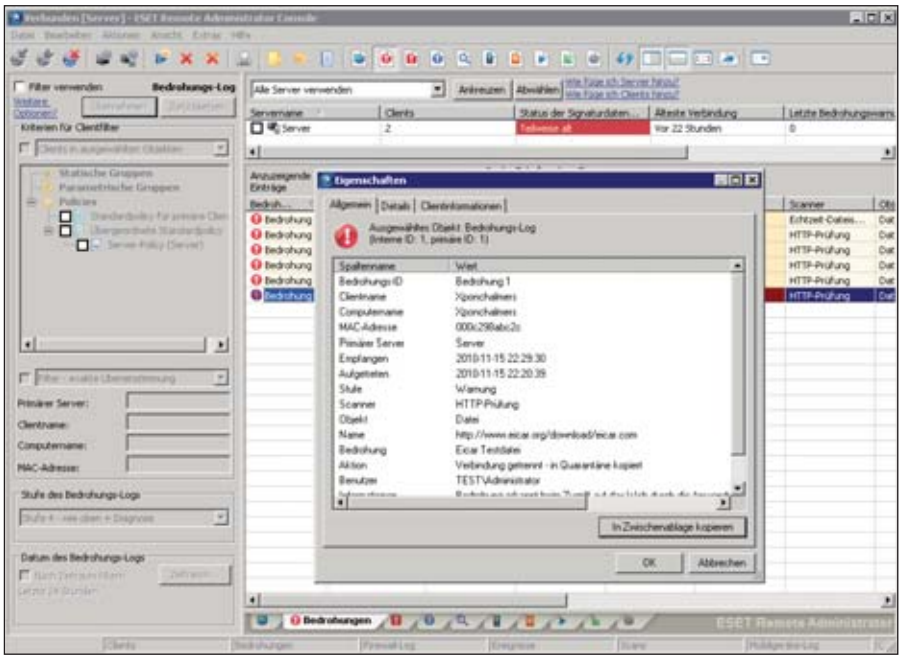


Bild 1: ESET liefert eine solide und übersichtliche Management-Oberfläche für seine Software mit

spielsweise über die Technik zum Versand von verdächtigen Elementen an spezielle, im Internet gehostete Server, so durfte die AV-Software dies auch in der Teststellung nutzen, um das Ergebnis zu optimieren. Der Trend der AV-Hersteller hin zu einer verstärkten Nutzung der "Cloud-Technologie" ist unübersehbar. Dies hat Auswirkungen auf die Parametrierung. Administratoren sollten künftig davon ausgehen, dass Antivirenserver viel häufiger größere Datenmengen mit dem Internet austauschen.

Rubrik 3, die so genannte "Wildlist" [3], lieferte für alle sechs Testkandidaten ein absolut identisches Ergebnis. Alle 5.084 Schädlinge – sowohl einmal per On-Demand-Scanner als auch einmal mit dem On-Access Virenwächter geprüft – wurden von jeder Lösung zu 100 Prozent erkannt. Dass ausgerechnet dieser Test ein so phantastisches Ergebnis erfährt, erklärt sich dadurch, dass Schädlinge, die auf der "offiziellen Wildlist" stehen, von allen Herstellern garantiert erkannt werden, da sie die notwendige Datenquelle gemeinschaftlich mit Informationen füttern. Somit ist beinahe ausgeschlossen, dass eine professionelle AV-Lösung diese digitalen Plagegeister nicht entdeckt. Bedingt durch das einheitlich gute Ergebnis in dieser eher unrealistischen Disziplin verzichteten wir darauf, diese Ergebnisse in die Kalkulation der Leistung einzubeziehen.

Die vierte Testrubrik widmet sich dem Thema der Performance. Es liegt auf der Hand, dass eine Schutzsoftware, die alle Dateien und Prozesse genau überwacht, dafür Zeit benötigt. Im Performance-Test wird die zeitliche Auswirkung in verschiedenen Verfahren geprüft. Dabei wurden typische Vorgänge eines Benutzers wie PC starten, Word öffnen, Dateien bearbeiten oder Webseitenzugriffe gemessen. Während einige Testbereiche nur minimale Verzögerungen beim Einsatz einer AV-Lösung offenlegten, kam es in anderen Tests zu teilweise dramatischen Verlangsamungen.

ESET Smart Security 4

Von ESET, unter anderem bekannt für NOD32 Antivirus, stammt eine typische Antivirenlösung für den Unternehmenseinsatz. Auch wenn der Name möglicherweise dazu verleitet, etwas anderes zu denken, so ist die Software durchaus x64-fähig. Neben allen Windows-Servervarianten unterstützt NOD32 Linux und BSD/Solaris-Betriebssysteme jeweils in der 32- und 64-Bit-Ausprägung. Apples Mac OS X wird ab Version 10.5 durch "ESET NOD32 Antivirus Business Edition für Mac" unterstützt, das derzeit noch im Public Beta Stadium befindlich ist. "ESET NOD32 Antivirus für Linux Desktop" soll zudem alle großen Distributionen wie Suse, Red Hat, Ubuntu mit eigenen Paketen und durch ein generisches Linux-Paket auch andere Distributionen unterstützen. Für Microsoft Outlook bietet der Hersteller ein spezielles Plug-In, das auf Virenbefall, Phishing-Versuche oder HTML-Infektion der E-Mail und des Anhangs prüft.

Alle Produkte für Client- und Serversysteme verwaltet der Administrator zentral über den "ESET Remote Administrator". Die Einrichtung besteht aus der eigentlichen Serversoftware, der Konsoleninstallation, die auch von beliebigen Rechnern im Netzwerk aus ausgeführt werden kann, sowie dem NOD32-Client, der auch auf dem Server installiert wird. Keines der MSI-Pakete verbraucht mehr als 45 MByte Speicherplatz. Der Administrator wird von einem Installationsassistenten geführt, der auch bei der Konfiguration einer ausfallsicheren Clusterinstallation hilft. Für unterschiedliche Dienste, wie beispielsweise Zugriff auf die Konsole, Lesezugriff auf die Konsole, Replikation oder Remote Installer, kann der Administrator schon zur Installation verschiedene Passwörter setzen. Datenbankseitig bringt der so genannte ERA-Server alles für den Betrieb im KMU-Umfeld Notwendige mit. Ist nicht mindestens Microsoft SQL 2005, MySQL 5.0 oder Oracle 9i am Standort vorhanden, so arbeitet ERA mit der integrierten Microsoft Access-Datenbank. Der Hersteller empfiehlt diese Form der Installation für Umgebungen mit einigen hundert Client-Systemen.

Sofern mehr als ein AV-Server im Netzwerk installiert wird, ist für Administratoren entscheidend, auf welche Weise sie die unterschiedlichen Maschinen ansteuern können. Üblicherweise wird eine Konfiguration gewählt, bei der von einer zen-

tralen Stelle aus alle Server auf einmal angesteuert werden können. Bei ESET geschieht dies über das zentrale Management Tool "ESET Remote Administrator". ESET-RA verfügt über die Möglichkeit, mehrere Serverdienste untereinander zu replizieren, und baut somit eine Kaskade von Servern. Die Konfiguration, Policies oder Tasks steuert der Administrator zentral über die Software und erhält auch alle Statusmeldungen von Computern und Servern in dieser Konsole. Je nach Konfiguration der Internetanbindung in verteilten Netzwerken sind Konstellationen im ESET Remote Administrator abzubilden, bei denen die Update-Pattern auf einem Server heruntergeladen werden und über den integrierten HTTP-Serverdienst an die untergeordneten Server verteilt werden.

In nur wenigen Unternehmen ist es möglich, eine einheitliche Richtlinie für den Virenschutz umzusetzen. Es gibt Server-Systeme und einzelne PCs, die beispielsweise nicht verändert werden dürfen. Darunter kann auch der Virenschutz fallen. Bei ESET ist die Bildung von unterschiedlichen Gruppen für verschiedene Richtlinien sehr einfach gelöst. Es gibt sowohl statische Gruppen, die manuell gepflegt oder mit dem Active Directory synchronisiert werden, aber auch Gruppen, die sich anhand von Kriterien dynamisch zusammensetzen.

Die Verteilung der Client-Installation geschieht entweder über die Einbindung der MSI-Pakete in eine professionelle Softwareverteilung oder direkt über das ESET Remote Administrator-Interface. Domänen-Rechner werden in der Auflistung automatisch dargestellt und dank der Möglichkeit, verschiedene Anmeldeinformationen zu hinterlegen, ist eine Verteilung auch auf domänenfremden PCs möglich. Eine Testfunktion hilft bei der Eingrenzung von Fehlern, sofern sich Pakete nicht verteilen lassen. Sehr angenehm für den Administrator ist die gemeinschaftliche Einbindung der Installationspakete für x86- und x64-Windows. Der Installationsagent wählt dabei selbstständig die passende Variante aus.

Hersteller
ESET
www.eset.de

Preis
Preis für 100 Windows-Clients, Server, 120 Mailboxen, Remote-Admin: 2.769,75 Euro

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

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

Erkennungsrate Web-Attacken	9
Erkennungsrate Malware	6
Handhabung / Management	8
Installation und Client-Unterstützung	8
Leistung	9
Gesamtbewertung	**8**

ESET Smart Security 4.2.64.12

Fazit

Im Test schlug sich ESET ordentlich. Von den 13 Attacken durch Webseiten verhinderte die Software das Öffnen der Webseite in zwölf Fällen und in einem Fall wurde der Schädling nach dem Öffnen der Webseite erkannt und eliminiert. Somit wurde der Benutzer von diesem Angriff gänzlich verschont. Von den 201.940 unterschiedlichen Malware-Vertretern erkannte die Software lediglich 94 Prozent, das zweitschlechteste Ergebnis in unserem Test. Besonders gut erkannte ESET Smart Security Würmer mit 99,69 Prozent und Viren mit 98,92 Prozent. Schlechter sah es indes in der Kategorie der potenziell unerwünschten Programme aus, die mit nur 91,58 Prozent Erkennungsrate das schlechteste Ergebnis im Testfeld bildet – möglicherweise werden solche Dateien absichtlich nicht erkannt, um rechtliche Probleme zu vermeiden. Die Performance-Werte sind insgesamt überzeugend, lediglich das Kopieren einer Auswahl von Dateien über das Netzwerk verlangsamte sich im Vergleich zu einem ungeschützten PC um etwas mehr als die Hälfte.

AVG Internet Security Business Edition 2011

AVG besteht als Unternehmen bereits seit 1991 und hat sich auf Sicherheitssoftware spezialisiert. Gänzlich neu im Funktionsumfang ist die "Protective Cloud-Technologie". Diese Technologie nutzt gleichzeitig verschiedene Scan-Engines und Verhaltenserkennung, um aufkommende und bisher unbekannte Bedrohungen zu identifizieren. Nachdem eine Bedrohung erkannt wurde, will der Hersteller zeitnah Abwehrmittel entwickeln und die AVG-Clients aktualisieren. Neben dem Abgleich mit der Internetdatenbank als "Cloud-Computing"-Technik bietet die Software die bekannten Suchmethoden über Signaturen, Heuristiken sowie Generiken und wertet das Verhalten von Programmen aus. Somit ist ein Schutz vor Schadsoftware auch dann gewährleistet, wenn Rechner keinen Zugriff auf das Internet haben.

Für den Unternehmenseinsatz bietet der Hersteller zwei Editionen. Die "AVG Anti-Virus Business Edition" bietet den Virenschutz auf Workstations und Fileservern und ist somit eine klassische Antivirensoftware. Die aktuelle "Internet Security Business Edition" bietet darüber hinaus Spam-Schutz für E-Mail-Clients und eine zentral zu verwaltende Firewall. AVG beschränkt sich bei der Produktunterstützung auf aktuelle Windows-Versionen. Zwar bietet AVG kostenfreie AV-Lösungen für Mac OS und Linux an, beide sind jedoch nicht für ein zentrales Management geeignet.

Die Installation der Server-Software ist sehr einfach. Nach einem Doppelklick auf den Installer ist lediglich die Eingabe einer Lizenznummer notwendig. AVG bietet, wie viele andere Hersteller auch, nunmehr eine Erweiterung für den Browser in Form einer "Security Bar" an. Bisher waren in erster Linie kostenlose Programme durch diese mehr oder minder sinnvolle Erwei-

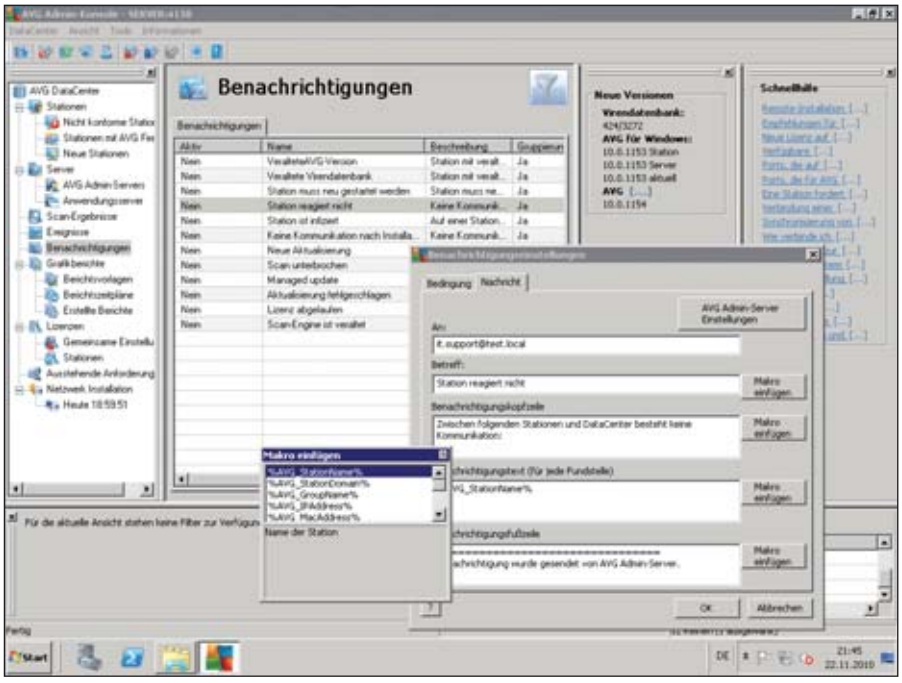


Bild 2: Wie Administratoren über Missstände informiert werden, ist bei AVG sehr genau steuerbar

terungen aufgefallen. Gemäß der guten Gepflogenheit, auf Server so wenig Software wie notwendig einzuspielen, verzichteten wir auf dieses Add-On. Die komplette Installation des 178 MByte großen Installers dauerte auf dem Testsystem keine zwei Minuten. Direkt nach der Einrichtung versorgte sich die Software automatisch mit aktuellen AV-Pattern.

Um mit der AVG-Lösung zentral Clients zu verwalten, ist die Installation der Remote Administration Console (RAC) erforderlich. Der Admin-Server-Implementierungsassistent unterstützt den Administrator bei der Einrichtung der beiden zur Verfügung stehenden Serverdienste. In der Testinstallation wählten wir sowohl die "DataCenter-Rolle" als zentrale Management-Oberfläche als auch die "UpdateProxy-Rolle", die Client-Computer mit Updates und AV-Pattern ausstattet. Die Rolle als Datacenter benötigt für den Betrieb eine Datenbank. Zur Auswahl stehen Firebird, Microsoft SQL und SQL Express, Oracle 10g oder 11g oder MySQL 5. Die Firebird-Datenbank für rund 150 Clients wird vom Assistenten auf Wunsch des Administrators automatisch eingerichtet. Der folgende Schritt des Assistenten führt den Administrator zur Übernahme von Client-Informationen. Ist bereits eine Installation vorhanden, so können aus einem Backup alle Informationen ausgelesen werden. Eine Verknüpfung zu einem Active Directory steht als weitere Option zur Verfügung.

Im Test verlief die Verteilung der Client-Software ohne Schwierigkeiten. PCs, die in der Domäne organisiert sind, lassen sich durch den Administrator über das aus Windows bekannte Domänenfenster suchen und für die Verteilung auswählen. Eine Gruppierung der Computer und Server über die Management-Konsole ist ebenfalls problemlos möglich. Eine Einteilung von Computern in Gruppen ist in jedem Unternehmen wichtig, in dem der Virenschutz oder andere Sicherheitsregeln feiner eingestellt werden sollen. Besonders einfach hat AVG die Aktualisierung der Installationspakete realisiert. Durch einen einzigen Mausklick lädt die Software aus dem Programmfenster heraus die neueste Version herunter. Um Details wie x64- oder x86-Version muss sich der Administrator dabei nicht kümmern – das übernimmt die Software automatisch. Ebenfalls für den Administrator sehr angenehm umgesetzt sind die Benachrichtigungsfunktionen. Die typischen zwölf Ereignisse, darunter "Station infiziert", "Scan unterbrochen" oder "Veraltete Virendatenbank", stehen zur Auswahl, um E-Mail-Benachrichtigungen an den IT-Support zu versenden. Je nach Ereignisart können verschiedene Werte eingestellt werden, bei deren Erreichen oder Unterschreiten die Nachricht versendet wird.

Fazit

Die AVG-Lösung lieferte im Test ein sehr gutes Ergebnis ab. Die 13 infizierten Webseiten wurden allesamt blockiert, ehe es zu einem Schaden auf dem Computer kommen konnte. 96,65 Prozent aller getesteten Schädlinge wurden erkannt und vernichtet. Das ist im Vergleich zur Konkurrenz ein insgesamt überzeugendes Ergebnis. Die Performance-Auswirkungen durch die Software liegen in einem vertretbaren Bereich. Lediglich das Kopieren

Hersteller
AVG
www.avg.com/de-de/

Preis
Für 100 Windows-Clients, Server, inklusive Mailserver mit 120 Mailboxen kostet AVG AV Business Bundle 1.929,87 Euro sowie AVG ESE für 120 Mailboxen 2.043,70 Euro.

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

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

Erkennungsrate Web-Attacken	10
Erkennungsrate Malware	8
Handhabung / Management	9
Installation und Client-Unterstützung	8
Leistung	7

Gesamtbewertung **8,4**

AVG Internet Security Business 10.0.1153

lokaler Dateien verlangsamt sich um die Hälfte und die Berechnung von MD5-Hashes für eine Auswahl von Dateien ist um 77 Prozent langsamer als ohne den Schutz. Insgesamt handelt es sich bei AVG um eine gut gelungene und ausgewogene Antivirus-Software.

Avira Antivir

Für den Unternehmenseinsatz bietet der deutsche Software-Hersteller Avira verschiedene Varianten seiner Produkte an. Auf den Clients installiert der Administrator über eine zentrale Management-Software auf Basis der Microsoft MMC 3.0 die "Professional Version". Server werden mit der entsprechenden "Server-Edition" ebenfalls über das "Security Management Center" (SMC) verwaltet. Bei der Installation des ersten Servers wird der Administrator befragt gegen welche Arten von Schädlingen die Maschine geschützt werden soll. In der Standardeinstellung sind Adware, Spyware, Backdoor, Phishing und Viren ebenso ausgewählt wie die in der deutschen Übersetzung etwas seltsam klingenden Varianten wie "Dateien mit verschleiernden Dateiendungen". Im nächsten Dialogfeld folgt eine Auflistung von Produkten, die vom "Guard" ausgelassen werden sollen – darunter das Active Directory und der Exchange Server. Der tiefere Sinn der Nichtbeachtung erschließt sich dem Programmneuling an dieser Stelle leider nicht. Auf Nachfrage erklärte der Hersteller, dass ein regelmäßiger Scan von großen Datenbankdateien eine sehr hohe Last erzeugen würde, ebenso verhält es sich bei Backupdateien. Zudem lässt sich über das bewusste Auslassen von Programmen verhindern, dass es zu irrtümlichen Virenfunden kommt. In Clusterumgebungen sollte der Scanner die für die Clusterfunktionalität entscheidenden Verzeichnisse ebenfalls auslassen. Insgesamt verlief die Installation der Software im Test sehr einfach und zügig.

Für verteilte Umgebungen, in denen es eine zentrale Serverinstallation gibt und AV-Pattern über WAN-Strecken an entfernte Orte übermittelt werden, empfiehlt sich der Einsatz des so genannten "Internet Update Managers (IUM)". Die Anzahl dieser Verteiler-Server ist nicht begrenzt und ermöglicht den Aufbau einer Kaskade von Verteil-Servern. Die Konfiguration selbst ist jedoch auf eine zentrale "SMC"-Konsole beschränkt. Untergeordnete Server, die nur einen Teil der Clients verwalten, sind innerhalb einer gemeinsamen Struktur nicht realisierbar. Der Aufbau unterschiedlicher Gruppen, beispielsweise für Server, die nicht automatisch aktualisiert werden sollen, ist indes möglich. Für jede Gruppe in der Konsole kann der Administrator bei Bedarf unterschiedliche Konfigurationseinstellungen wählen.

Dank der Filterfunktionen ist die Suche nach ungeschützten PCs im Netzwerk für den Administrator leicht durchführbar. Alle Client- und Serversysteme einer Domäne tauchen durch einen "Domänenimport" in der Ansicht auf. Rechner, auf denen ein Produkt nicht installiert ist, erscheinen in dem durch den Administrator zu erstellenden Filter.

Das Security Management Center von Avira hinterlässt im Test einen soliden und übersichtlichen Eindruck. Dank deutschsprachiger Oberfläche erklären sich alle Dialoge von allein. Die Benutzerverwaltung erlaubt dem Administrator das Anlegen verschiedener "Sub-Administratoren",

Performance-Einflüsse

Anbieter	XP Pro SP3	AVG	Avira	ESET	G Data	Kaspersky	McAfee
Produkt	Referenz-XP	AVG Internet Security Business Edition 2011	Avira AntiVir Professional	ESET Smart Security 4 Business Edition	G Data AntiVirus Enterprise 10	Kaspersky Anti-Virus 6.0	McAfee Total Protection for Endpoint
Programmversion	-	10.0.1153	10.0.0.937	4.2.64.12	10.7.1.112	6.0.4.1424 (a)	4.5.0.1270
Genutzter Speicher nach Systemstart in Kbyte							
Working Set	0,0	130.277,1	37.705,7	63.992,6	55.524,0	44.622,9	76.908,0
Private Virtual Memory	0,0	120.146,9	114.306,3	59.811,4	256.985,1	44.679,4	114.780,0
Private Virtual Memory Peak	0,0	167.376,6	275.252,0	95.308,0	328.014,3	219.620,6	128.618,3
Anzahl an Prozessen							
(min / max)	- / -	14 / 16	4 / 6	2 / 2	6 / 6	2 / 2	12 / 14
Startup / Shutdown-Zeiten (in Sekunden/Messabweichung)							
Kaltstart	47,68 / 0,56	61,05 / 0,08	48,37 / 0,05	48,61 / 0,10	50,23 / 0,22	51,24 / 0,18	93,28 / 0,11
Shutdown	9,01 / 0,09	17,78 / 0,19	11,39 / 0,24	9,51 / 0,08	10,00 / 0,12	12,86 / 0,24	13,76 / 0,16
Download von 20 PDF-Dateien aus dem Internet	3,59 / 0,09	6,26 / 0,09	5,30 / 0,19	6,80 / 0,08	4,38 / 0,16	9,82 / 0,13	6,20 / 0,09

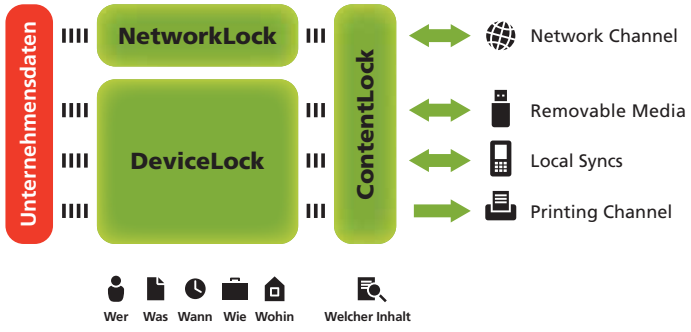
Macht kein großes Aufheben um ein paar Überstunden.

Oder um ein paar Datensätze.

Mitarbeiter sind auch nur Menschen.
Da kann es passieren, dass Daten unverschlüsselt in falsche Hände geraten. Oder gelöscht werden. Oder manipuliert. Oder mit Viren verseucht. Schützen Sie sich davor!

- Kontrolle sämtlicher PC-Schnittstellen, inkl. Webmail, FTP, Facebook & Co.
- Schutz vor Datenbeschädigung und -verlust durch Unachtsamkeit oder Vorsatz
- Individuelle Justierbarkeit
- Für kleine, große und größte Netzwerke
- Über 4 Mio. Installationen
- Referenzen in hochsensiblen Branchen
- Neu! Jetzt mit vollständiger Content- und Kontext-Prüfung

Die Datenflusskontrolle der DeviceLock Endpoint DLP-Suite



Informieren Sie sich jetzt!
www.devicelock.de oder wählen Sie die Nummer sicher: +49.2102.89211-0

[www.devicelock.de]

DeviceLock®
Proactive Endpoint Security

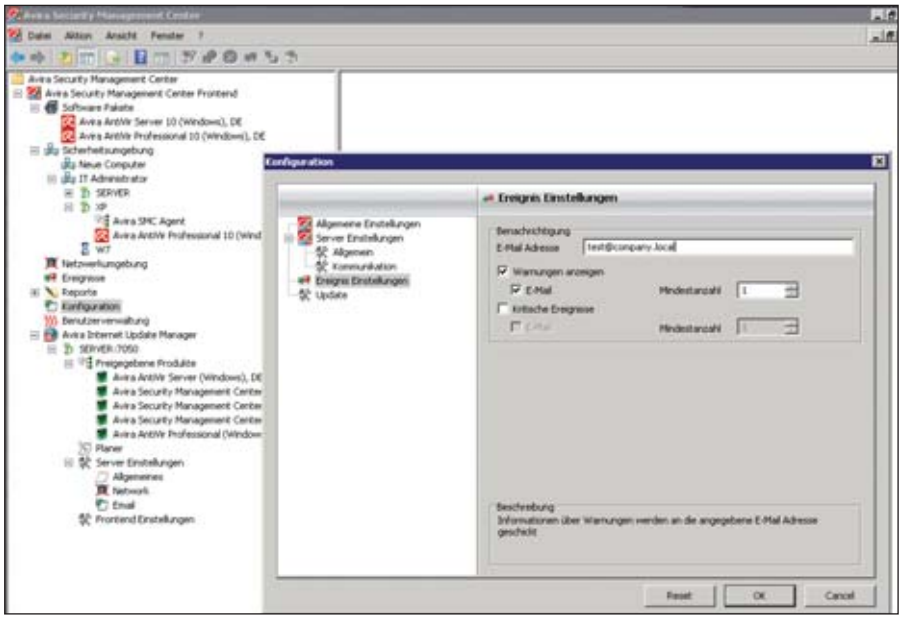


Bild 3: Im Vergleich zu den Marktbegleitern ist die Management-Oberfläche von Avira eher einfach in MMC-Gestalt gehalten

denen die zwölf vorgegebenen Rechte – von der Anzeige der Reports über das Löschen von Events bis zur Verwaltung von Software-Paketen – beliebig zugeordnet werden. Eine Gruppenbildung für Benutzer sieht die Software nicht vor. Ebenfalls eingeschränkt ist die Integration der Konsole in die weiteren Serverprodukte von Avira. Zwar bietet der Hersteller spezielle Lösungen für Microsoft SharePoint oder Microsoft Exchange, jedoch lassen sich diese Produkte, außer WebGate und Mailgate, nicht über die zentrale Konsole verwalten. Die Abbildung unterschiedlicher Mandanten ist ebenfalls nicht möglich.

Die Betriebssystemunterstützung von Avira ist löblich. Unix/Linux-seitig werden Red Hat Enterprise 4/5, Suse Linux 9-11, Debian 4/5, Ubuntu 8/9 und Sun Solaris 9/10 für SPARC unterstützt. Unter Microsoft Windows ist die Version 2000 SP4 UR1 oder höher erforderlich. Gemäß der Produktstrategie versorgt Avira eine Windows-Version noch ein Jahr nach deren endgültiger Abkündigung mit AV-Pattern und Programm-Updates.

Fazit

Die Testergebnisse bescheinigen dem Produkt eine insgesamt gute Note. Die Performance ist hervorragend, keine andere Software bremst den Computer weniger aus. Leider konnte die Software nur zehn der 13 infizierten Webseiten blockieren, in drei von 13 Fällen infizierte sich der PC mit einer Malware, ohne dass die Schutzsoftware darauf reagierte. Die Erkennungsrate von 98,60 Prozent aus den über 200.000 ausgewählten Schädlingen ist eine solide Leistung. Die Erkennungsrate bei den Backdoor-Programmen erreichte mit 99,55 Prozent den Maximalwert der Untersuchung.

G Data Antivirus Enterprise

AntiVirus Enterprise 10.7 wird von G Data als High-End-Virenschutz für Firmennetzwerke eingestuft. Über eine zentrale Management-Konsole steuert der Administrator die Konfiguration und das Geschehen für Mailserver, Fileserver, Desktop-Computer und Notebooks. Der Hersteller setzt bei der Suche auf ein Doppelgespann aus der BitDefender-Engine ergänzt durch die Scan-Technologie von Avast (Alwil). Wie die Marktbegleiter auch ergänzt G Data die Pattern-basierte Suche durch die heuristische Suche nach bisher unbekannten Viren und nutzt "Cloud Security", bei der fragliche Elemente durch im Internet betriebene Antiviren-Programme zusätzlich geprüft werden.

Bei der Downloadgröße stellt G Data den Rekord im Testfeld auf: Ganze 1,6 GByte umfasst der Installer, den der Hersteller für die komplette Lösung bietet. Angenehm zügig geht indes die Installation selbst vonstatten. Der G Data AntiVirus Management Server arbeitet mit einer integrierten Datenbank, die während des Installationsvorgangs automatisch eingerichtet wird, oder mit einer vorhandenen SQL-Server Instanz oder Microsoft SQL-Express. Ein separat eingerichteter SQL-Express Server wird für große Netzwerke empfohlen.

Die Registrierung der Software, selbst in einer Testinstallation, ist bei G Data Pflicht. Ohne sie verweigert das Programm das Herunterladen von AV-Pattern und Programm-Updates. Die Login-Informatio-

Hersteller
Avira
www.avira.de

Preis
Für 100 Windows-Clients, Server, inklusive Mailserver mit 120 Mailboxen kostet das Network Bundle für 100 Benutzer 3.177,30 Euro.

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

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

Erkennungsrate Web-Attacken	7
Erkennungsrate Malware	8
Handhabung / Management	8
Installation und Client-Unterstützung	10
Leistung	8

Gesamtbewertung **8**

Avira AntiVir Professional 10.0.0.937

nen für den Update-Server werden im Zuge der Installation angezeigt. Leider hat dieses Fenster keine Möglichkeit, die Daten zu speichern – wohl aber eine Checkbox mit der Bestätigung: "Ich habe die Daten abgeschrieben".

Nach der ersten Anmeldung, die administrative Login-Daten des Servers oder der Domäne erfordert, wird der Administrator von einem Konfigurationsassistenten begrüßt. Die aktuellen Clients und Server in der Domäne werden sofort aufgelistet und ehe sich der Benutzer auch nur ein einziges Mal auf der Oberfläche umgeschaut hat, kann die Verteilung der Antiviren-Lösung eingerichtet werden. Computer, die nicht auf der Liste aufgeführt sind, lassen sich durch Eingabe des Rechnernamens ebenfalls sofort für die Aktivierung vorsehen. Die kontextsensitive Onlinehilfe in deutscher Sprache beantwortet die Fragen des Administrators, ohne diesen mit zu großen Texten zu überschütten.

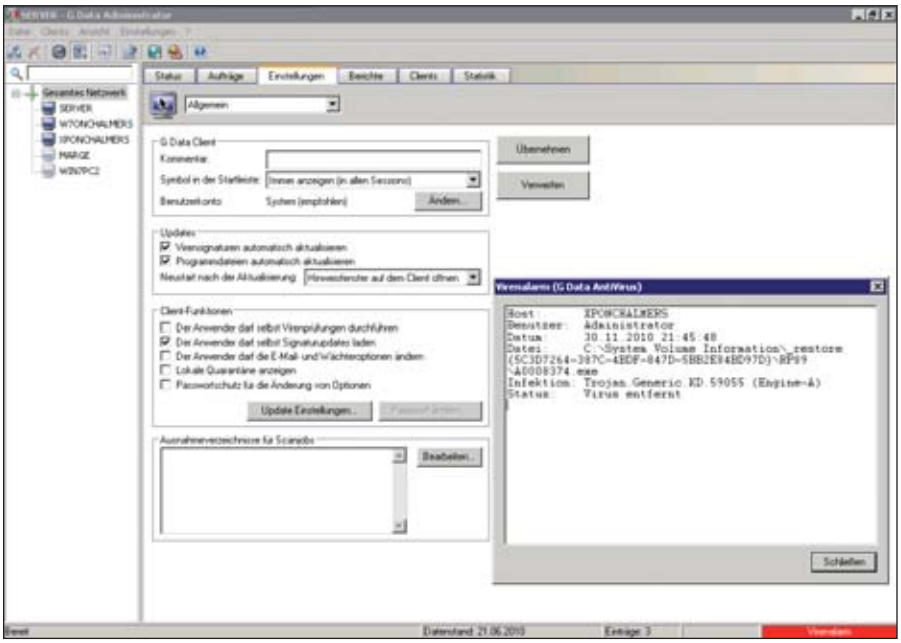


Bild 4: Schlicht und funktionell: die Management-Oberfläche von G Data

AntiVirus Enterprise 10.7 ging ohne Neustart faktisch sofort zum Einsatz über. Die schon während der Erstkonfiguration ausgewählten Client-Rechner wurden in weniger als drei Minuten mit der Client-Software ausgestattet. Die Übersichtsanzeige in der Konsole monierte quasi in Echtzeit, dass die Virensignaturen nicht mehr auf dem neuesten Stand waren. Klickt der Administrator auf die Meldung, so erscheint die Liste der nicht mehr aktuellen Rechner in einem kleinen Zusatzfenster. Aus diesem Fenster ist eine manuelle Aktualisierung mit einem Mausklick möglich.

Alle weiteren Einstellungen – von der Alarmmeldung an den Administrator über periodische Aktualisierungen der Signaturen auf dem Server und den Clients hin zur Definition von Scan-Ausnahmen – sind bei G Data absolut selbsterklärend in den Dialogen vorzunehmen. Ohne größere Anstrengungen ist eine zusätzliche Gruppe eingerichtet, bei der sich die zugeordneten Client-Computer ihre Updates nicht über den Management-Server herunterladen, sondern das "Internet-Update selbst durchführen". Eine weitere Option bei G Data ist "Internet-Update bei veralteten Virensignaturen selbst durchführen, wenn keine Verbindung zum Management-Server hergestellt werden kann". Dies ist beispielsweise dann sinnvoll, wenn Notebooks für Außendienstmitarbeiter nur selten mit dem Firmennetzwerk direkt verbunden sind. Clientseitig arbeitet die Software unter Windows 2000 oder höher.

Für beide AV-Engines bietet G Data im Menü eine spezielle Rollback-Funktion an. Neben dem bewussten Zurücksetzen der AV-Signaturen auf ein älteres Datum ist eine Sperrung der Updates bis zu einem frei definierbaren Datum möglich. Möchte der Administrator beispielsweise sicherstellen, dass sich Client-Computer in einem bestimmten Zeitfenster unter keinen Umständen aktualisieren, so ist dies bei G Data mit wenigen Mausklicks erledigt.

Trotz sehr guter Management-Oberfläche und einem Doppelgespann der Such-Engines erlaubte sich G Data im Praxistest ein paar Schwächen. Von den 13 infizierten Webseiten wurden die Infektionen nur von sechs Seiten verhindert. In einem Fall erkannte der Scanner nachträglich, dass eine infektiöse Datei auf dem Client-PC begann, ihr Unwesen zu treiben. Von den

Hersteller
G Data
www.gdata.de

Preis
Für 100 Windows-Clients, Server, inklusive Mailserver mit 120 Mailboxen beträgt der Preis bei 12 Monaten Laufzeit 1.872 Euro.

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

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

Erkennungsrate Web-Attacken	4
Erkennungsrate Malware	9
Handhabung / Management	9
Installation und Client-Unterstützung	8
Leistung	8
Gesamtbewertung	**7,6**

G Data AntiVirus Enterprise 10

anderen sechs Webseiten wurde der Computer ungehindert attackiert und infiltriert. Für die Erkennungsrate der Auswahl von 201.940 Schädlingen erhielt G Data indes die Bestnote. Mit einer Erkennungsrate von 99,84 Prozent ist G Data in dieser Rubrik der Testsieger.

Für die Performance des Systems hat der Einsatz der doppelten Suchfunktion üblicherweise keine sehr großen negativen Auswirkungen. Nur in äußerst theoretischen Tests, beispielsweise der Erstellung von 10.000 Dateien mit exakt identischem Inhalt, fiel eine äußerst schlechte Leistung auf. Während der Standard-PC ohne Virenschutz für die Erledigung dieser Aufgabe lediglich 156 Sekunden benötigt, sind es unter G Data Antivirus 1.354 Sekunden. Dieser starke Ausreißer deutet auf einen Fehler im Programm hin. Das Öffnen des Internet Explorers nach einem Neustart verlangsamt sich jedoch auf spürbare 6,64 Sekunden, im Vergleich zu 2,79 Sekunden ohne Virenschutz. Einen weiteren Ausreißer liefert sich das Programm bei der Komprimierung von Dateien mit WINRAR, wobei sich die Leistung des PCs um spürbare 32 Prozent verringerte.

Fazit

Während die Administration von G Data Antivirus Enterprise vorbildlich gelöst ist, konnte das Resultat der Scans in unserem Test nicht so recht überzeugen. Lediglich in der Erkennung von Schädlingen glänzte das Antiviren-Programm. Erfreulich war ebenfalls, dass trotz der Doppel-Engine sich die Scanzeiten in Grenzen hielten. Bleibt zu hoffen, dass G Data mit der für Frühjahr 2011 geplanten neuen Version mit seinen Schwächen aufräumt.

Kaspersky Anti-Virus 6.0

Kaspersky bietet ein breit aufgestelltes Portfolio an verschiedensten AV-Lösungen an. Für den Einsatz im KMU-Umfeld empfiehlt der Hersteller Anti-Virus 6.0 für Server und Workstations in Zusammenarbeit mit dem Administration Kit. Sehr praktisch ist eine Einstellung des Installers bei der Einrichtung des Servers: Eine Checkbox bietet an, die von Microsoft empfohlenen Datenbereiche für den Scanner auszuschließen. Noch ehe der erste Server eingerichtet ist, steht eine Aktualisierung der Programm- und Antivirendateien direkt über das Inter-

Die Scanresultate im Überblick

Produkt		AVG Internet Security Business Edition 2011	Avira AntiVir Professional	ESET Smart Security 4 Business Edition	G Data AntiVirus Enterprise 10	Kaspersky Anti-Virus 6.0	McAfee Total Protection for Endpoint
Programmversion		10.0.1153	10.0.0.937	4.2.64.12	10.7.1.112	6.0.4.1424 (a)	4.5.0.1270
Webseiten-Attacken							
Vollständig blockierte Malware	von 13	13 / 100%	10 / 76,92%	12 / 92,31%	6 / 46,15%	10 / 76,92%	2 / 15,38%
Teilweise blockierte Malware	von 13	0 / 0%	0 / 0%	1 / 7,69%	1 / 7,69%	0 / 0%	3 / 23,08%
Nicht blockierte Angriffe (das System wurde infiziert)	von 13	0 / 0%	3 / 23,08%	0 / 0%	6 / 46,15%	3 / 23,08%	8 / 61,54%
Zoo Malware							
Summe	201.940	195.168 / 96,65%	199.119 / 98,60%	189.805 / 93,99%	201.613 / 99,84%	194.054 / 96,09%	179.885 / 89,08%
Malware							
Backdoors	15.067	14.850 / 98,56%	14.999 / 99,55%	14.008 / 92,97%	15.050 / 99,89%	14.717 / 97,68%	13.172 / 87,42%
Bots	4.405	4.317 / 98,00%	4.377 / 99,36%	4.260 / 96,71%	4.403 / 99,95%	4.292 / 97,43%	3.826 / 86,86%
Viren	10.515	10.387 / 98,78%	10.377 / 98,69%	10.401 / 98,92%	10.515 / 100,00%	9.957 / 94,69%	10.403 / 98,93%
Würmer	15.076	14.975 / 99,33%	15.048 / 99,81%	15.030 / 99,69%	15.070 / 99,96%	15.029 / 99,69%	14.760 / 97,90%
Trojaner							
Downloader	13.561	13.430 / 99,03%	12.817 / 94,51%	13.226 / 97,53%	13.549 / 99,91%	12.561 / 92,63%	12.176 / 89,79%
Dropper	5.155	4.983 / 96,66%	5.136 / 99,63%	4.855 /94,18%	5.150 / 99,90%	5.126 / 99,44%	4.314 / 83,69%
Generic	110.929	105.549 / 95,15%	109.338 / 98,57%	101.776 / 91,75%	110.679 / 99,77%	105.735 / 95,32%	96.187 / 86,71%
Passwort-Diebstahl-Programme	7.379	7.251 / 98,27%	7.297 / 98,89%	6.975 / 94,53%	7.364 / 99,80%	7.134 / 96,68%	6.349 / 86,04%
Andere Malware							
Unerwünschte Programme (PUA)	6.081	5.738 / 94,36%	5.969 / 98,16%	5.569 / 91,58%	6.062 / 99,69%	5.768 / 94,85%	5.657 / 93,03%
Rogue Applications (e.g. Fake AV)	13.772	13.688 / 99,39%	13.761 / 99,92%	13.705 / 99,51%	13.771 / 99,99%	13.735 / 99,73%	13.041 / 94,69%
Erkennung von Schädlingen aus der WildList							
	10.168	10.168 / 100%	10.168 / 100%	10.168 / 100%	10.168 / 100%	10.168 / 100%	10.168 / 100%

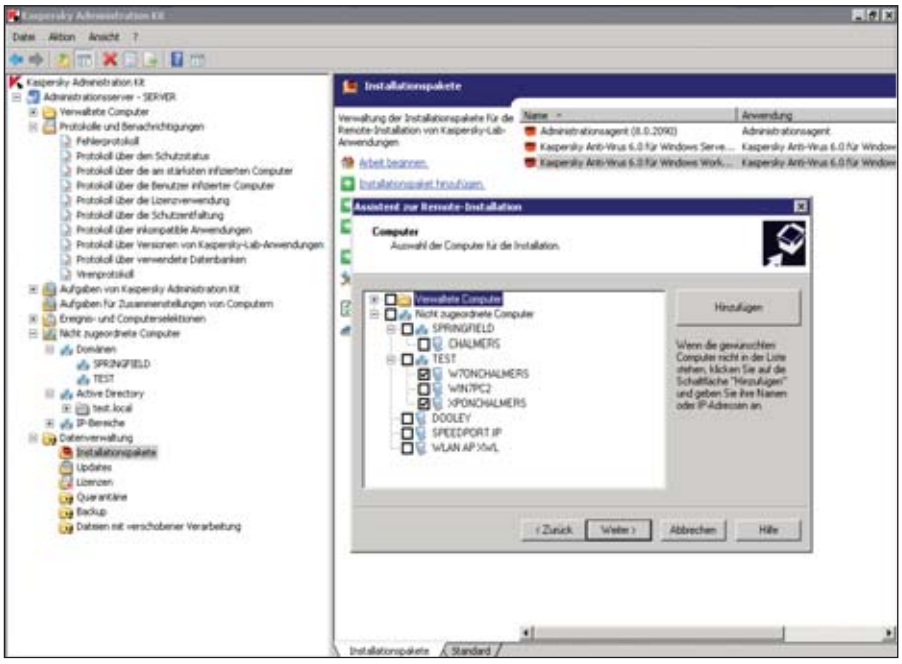


Bild 5: Die Steuerungsmöglichkeiten von Kaspersky Antivirus sind sehr umfangreich

Hersteller
Kaspersky Lab
www.kaspersky.com/de

Preis
Für 100 Windows-Clients, Server, inklusive Mailserver, 120 Mailboxen kostet "Kaspersky Enterprise Space Security" 3.542,34 Euro.

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

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

Erkennungsrate Web-Attacken	7
Erkennungsrate Malware	8
Handhabung / Management	10
Installation und Client-Unterstützung	9
Leistung	6
Gesamtbewertung	**8**

Kaspersky Anti-Virus 6.0.4.1424(a)

net an. Dieser Vorgang dauert zwar einige Minuten, stellt jedoch sicher, dass die Maschine von der ersten Sekunde an auf dem aktuellsten Stand ist. Ebenfalls bereits zur Installation des ersten Servers hat der Administrator die Möglichkeit, Regelwerke zur Untersuchung wie "Schnelle Suche" zwei Minuten nach dem Systemstart und die tägliche Komplettsuche zu aktivieren.

Bei der Installation des "Administration Kits", der zentralen Verwaltungssoftware von Kaspersky, wird der Administrator weit weniger mit technischen Details überschüttet. Im Gegensatz zu den Marktbegleitern fragt der Kaspersky-Installer nach der zu erwartenden Anzahl von Clients, anstelle Datenbankvarianten zur Auswahl anzubieten. Je nach Auswahl wird eine Microsoft SQL-Express oder File-basierte Jet-Datenbank eingerichtet. Fehlende Komponenten, beispielsweise Microsoft MDAC, lädt der Installer direkt über das Internet ohne Zutun des Administrators herunter und richtet sie ein. Ebenfalls sehr schön geregelt ist die Verhaltensweise zum Neustart der Client-Computer – der Administrator kann den Neustart nach Installation der Client-Software erzwingen, den Neustart auslassen oder den Benutzer befragen.

Die Einstellungsmöglichkeiten bei Kaspersky sind hervorragend. Unterschiedliche Gruppen, Abbildung von Mandantschaften, Aufbau von Kaskaden für Update-Server, Unterstützung von Linux- und Mac OS-Clients über das Administration-Kit, Benachrichtigung über E-Mail und SNMP dürften so ziemlich jeden Administrator-Wunsch erfüllen. Wird beispielsweise die Administrationssoftware auf einem Server deinstalliert, so bietet das Programm an, von den Einstellungen ein Backup zu erstellen, das auf einer anderen Maschine eingespielt werden kann. Dies ist äußerst praktisch, wenn es darum geht auf eine anderen Server umzuziehen.

Fazit

Kaspersky Anti-Virus überzeugte im Test als stabile Lösung. Die schlechten Performance-Leistungen trüben die Arbeit mit dem durch Kaspersky geschützten PC. Während der Download von 20 ZIP-Archivdateien üblicherweise 3,35 Sekunden Zeit veranschlagt, dauerte derselbe Vorgang unter Kaspersky AV 10,17 Sekunden. Während die Erkennung von Malware mit 96,09 Prozent gerade noch einen akzeptablen Wert darstellt, patzt das russische Softwarehaus beim Webseiten-Test. Drei von 13 infizierten Webseiten infizierten den Computer im Test, ohne dass die AV-Lösung darauf aufmerksam wurde.

McAfee Total Protection

Die Installation der Management-Software von McAfee, der "ePolicy Orchestrator 4.5", auf dem Windows Server 2008 R2 Testserver beginnt zunächst mit einer skurrilen Meldung, dass zunächst das 8.3-Benennungsschema zu aktivieren sei. Dazu muss ein Registry-Wert manuell umgesetzt werden. Warum das durch den Installer nicht durchgeführt wird, bleibt unklar. Die in der Dokumentation benannte automatische Installation eines Microsoft SQL Server Express nahm der Installer nicht vor und die Datenbank musste manuell eingerichtet werden. Keine Antivirenlösung im Test erforderte einen Neustart – lediglich McAfee verlangte diesen. Während die Konkurrenz innerhalb einiger Minuten ein-

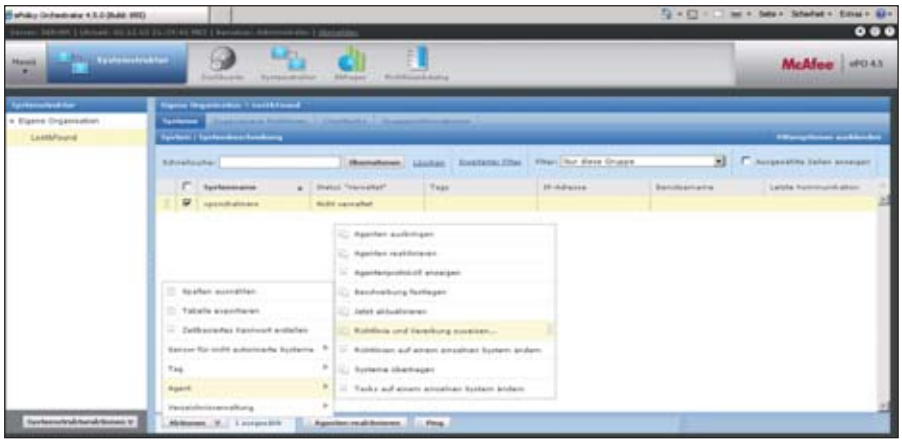


Bild 6: McAfee ist es bereits gelungen die komplette Management-Oberfläche auf Webtechnologie umzusetzen

gerichtet war, dauerte die McAfee Installation um ein Vielfaches länger.

Hat der Administrator die Hürden der komplizierten Einrichtung hinter sich gebracht, so erlebt er die Management-Oberfläche von McAfee insgesamt als moderne und leistungsfähige Software. McAfee ist der einzige Hersteller im Test, der eine Weboberfläche konsequent für die Steuerung seiner Antiviren-Lösung umgesetzt hat und bietet alle gebräuchlichen Funktionen von der Verteilung von Client-Komponenten über E-Mail-Benachrichtigung bis zur Gruppenbildung. Der Aufbau einer komplexeren Kaskade bei der Verteilung von AV-Pattern und Software-Paketen ist problemlos möglich. Die Einarbeitung in die Weboberfläche verlangt ein wenig mehr Aufmerksamkeit als bei der Konkurrenz. Bis erst einmal eine Übersicht über die aktuellen Rechner im Netzwerk sichtbar ist, vergehen einige Minuten bei der Suche nach den eher kleinen Menübefehlen, die sich untypisch im unteren Fensterbereich finden. Von den ansonsten guten und modernen Management-Fähigkeiten profitiert der Administrator angesichts der sonstigen Testergebnisse jedoch kaum.

Die Testergebnisse von McAfee Total Protection sind im Vergleich zu den Mitbewerbern insgesamt vernichtend. Acht von 13 Webattacken verliefen für die Malware erfolgreich – zum Nachteil für den Benutzer. Nur in zwei Fällen blockierte die Software, in drei Fällen reagierte erst der Scanner auf die Attacke. Die Erkennung von sonstigen Schädlingen liegt bei unter 90 Prozent, somit hat einer von zehn Schädlingen die Chance, das System zu infiltrieren. Als Ausweg bleibt die Erhöhung der Sicherheitseinstellung für alle Client-Systeme mit den entsprechenden Auswirkungen auf die Leistung. Leider sind die Performance-Daten schon in der Standardkonfiguration eher ernüchternd. McAfee ist in elf von 26 Tests das Schlusslicht und verzögert den Windows-Systemstart von 47,68 auf 93,28 Sekunden.

Fazit

McAfee bildete unter den sechs Antivirus-Suiten das Schlusslicht. Die Management-Oberfläche kommt zwar gut weg und basiert vollständig auf Webtechnik. Doch die eher komplexe Installation und vor allem die überschaubaren Erkennungsraten bescheren Total Protection den letzten Platz im Vergleichstest.

Gesamtfazit

Administratoren haben in Bezug auf Antivirus-Suiten die Qual der Wahl – und das ist auch gut so. Denn damit lässt sich das beste Produkt für den eigenen Bedarf auswählen. In unserem Vergleichstest haben alle Suiten ihre Vorzüge und auch Schwächen offenbart. Während fünf Produkte bei den Scan-Resultaten quasi gleichauf lagen, musste sich der preisgünstigste Anbieter McAfee hier geschlagen geben. Insbesondere der immer beliebtere Angriffsvektor Browser offenbarte deutliche Unterschiede zwischen den Kontrahenten. Nicht ganz aus dem Blick verlieren sollte der Administrator auch die Performance-Einbußen durch die arbeitenden Scanner. Besonders der Kaspersky-Scanner verlangsamte den Download von Dateien. Für intensive Online-Nutzer ist dies bedenklich. Doch alles in allem zeigten sich die Suiten durchaus robust und administrierbar. Und wie die Leistungen nach dem nächsten regelmäßigen Versionsupdate aussehen, steht ohnehin auf einem anderen Blatt. *(dr)*

Hersteller
McAfee
www.mcafee.de

Preis
Für 100 Windows-Clients, Server, inklusive Mailserver (Mail-Accounts) kostet McAfee Total Protection 989,60 Euro.

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

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

Erkennungsrate Web-Attacken	3
Erkennungsrate Malware	5
Handhabung / Management	8
Installation und Client-Unterstützung	6
Leistung	4
Gesamtbewertung	**5,2**

McAfee Total Protection 4.5.1270

Links

[1] Marktanalyse OPSWAT
B2T21
[2] AV-Test.org
B2T22
[3] Wildlist
B2T23

Strong Authentication mit dem Handy

SieMatic sichert Remote-Zugänge mit SMS PASSCODE

Bei SieMatic haben Hardware-Token zur Anwender-Identifikation bald ausgedient. Der traditionell innovative Küchenhersteller sichert seine Remote-Zugänge mit SMS PASSCODE ab und spart damit die Kosten für Authentisierungs-Geräte und Deployment. Der Anwender erhält ein Einmal-Password als Kurznachricht auf sein Handy. Dabei nutzt das Unternehmen seine Blackberry-Infrastruktur. "Authentisierung per Handy ist der neue Trend", bestätigt auch Robert Korherr, Marketingleiter beim Anbieter ProSoft.

Keine Alternative: Die Produktdaten der eleganten SieMatic-Küchen werden mit SMS PASSCODE abgesichert.

"Perfekt ist etwas nicht, wenn man nichts mehr hinzufügen kann, sondern wenn man nichts mehr weglassen kann." Nach diesem Motto erfand SieMatic vor fünfzig Jahren die griffl ose Küche. Im Weglassen übt man sich bei SieMatic auch bei einem neuen Authentisierungskonzept: Man setzt auf bestehende Hardware statt auf teure Token.

Sichere Remote-Zugänge

Dass auch jede Küche genau passt, dafür sorgt man im SieMatic-Rechenzentrum in Löhne. Dort werden unter anderem die Aufträge von Händlern und Vertriebspartnern in CAD-Vorlagen für die individuelle Küchenproduktion umgesetzt.

Etwa 75 Remote-Zugänge gibt es bei SieMatic derzeit. Sie werden für den Outlook-Web-Access genutzt sowie für das Portalsystem MS SharePoint, wo zum Beispiel Lieferanteninformationen oder Umsatzlisten bereitgehalten werden. Von außen ist auch eine CRM-Datenbank des Unternehmens zugänglich. Hier können die Mitarbeiter Marketing-Informationen einsehen und Verkaufsmöglichkeiten ausloten.

Wie heute allgemein üblich, werden auch bei SieMatic die Unternehmensdaten mit Strong Authentication abgeschirmt. Für die Mehrfaktor-Authentisierung waren bisher Hardware-Token im Einsatz. "Das war aber nicht die optimale Lösung," weiß Thorsten Pawelczyk, Leiter IT bei SieMatic. "Zum einen ist das Rollout an die Anwender aufwändig. Zum anderen haben die Token nur eine beschränkte Lebensdauer." Auch die Kosten sprachen gegen das etablierte Verfahren.

Blackberry statt Token

Die Token waren ohnehin überholt, im Unternehmen gab es nämlich schon einen zuverlässigen, geschützten Informationskanal. "Wir haben in eine komplette Blackberry-Infrastruktur investiert", erklärt Thorsten Pawelczyk, "inklusive Enterprise-Server".

Da lag es nahe, die mobilen Endgeräte auch für die SMS-Authentisierung einzusetzen. Mehr durch Zufall stieß man dabei auf SMS PASSCODE 4. Dieses Authentisierungs-System schickt jedem Anwender im Rahmen des Login-Prozesses ein Einmal-Passwort auf eine im System hinterlegte Handy-Nummer. Es ist nur kurze Zeit gültig und kann nur einmal verwendet werden. SMS PASSCODE prüft beim Login auch die Session-ID, sodass sich niemand unbemerkt in den Informationsfluss einklinken kann.

Sicher arbeiten im Home Office

So wurde auch bei SieMatic ein SMS PASSCODE Authentisierungs-Server installiert, außerdem ein Modem für den SMS-Versand. SMS PASSCODE 4 arbeitete bei SieMatic von Anfang an störungsfrei. "Der Server läuft sehr stabil. Besonders unsere amerikanischen Mitarbeiter nutzen das neue System sehr intensiv im Home Office", freut sich Thorsten Pawelczyk.

Das SieMatic Rechenzentrum plant einen weiteren Ausbau des Systems. Dann wollen die Admins auch noch einen Backup-Server an einem weiteren Standort installieren, Zweitmodem inklusive. Dazu bietet SMS PASSCODE sogar eine komplette Failover-Infrastruktur, bei der sich zwei Server gegenseitig überwachen.

Insgesamt also ein sehr stimmiges Gesamtsystem – auch für SieMatic: Auf die Frage, ob er auch nach Alternativen zu SMS PASSCODE gesucht habe, entgegnet Pawelczyk, "Haben wir, aber da gibt es zurzeit keine!"

ProSoft
MANAGE, SECURE, OPTIMISE IT.

ProSoft Software Vertriebs GmbH
Bürgermeister-Graf-Ring 10
82538 Geretsried
Tel. +49 8171-405-0
Fax + 49 8171-405-400

info@prosoft.de

Ansprechpartner:
Robert Korherr

Im Test: Lumension Patch and Remediation 7.0

Vielseitiger Flickschuster

von Jürgen Heyer

Mehrere hundert Sicherheitslücken werden jedes Jahr von den großen Softwareanbietern bekannt gegeben. Umso wichtiger ist eine konsequente Überwachung der Patchstände aller Systeme, um nicht Opfer eines Schadcodes zu werden, der diese Lücken ausnutzt. Eine sehr breite Abwehrbasis nicht nur für Windows-Schwachstellen bietet Patch and Remediation 7.0 von Lumension. Im Test hat sich IT-Administrator die Möglichkeiten der Software einmal genauer angesehen.

Lumension Security entstand 2007 aus dem Zusammenschluss von Patchlink und SecureWave. Ein zentrales Produkt ist die Lumension Endpoint Management and Security Suite (LEMSS), die aus drei Modulen besteht: Endpoint Power Management, Security Configuration Management und Patch and Remediation, das wir hier eingehender betrachten wollen. Im Gegensatz zu vielen anderen Patch-Werkzeugen, die sich ausschließlich auf – in den meisten Sicherheitsüberlegungen wohl im Mittelpunkt stehenden – Microsoft-Produkte konzentrieren, unterstützt Patch and Remediation neben den Windows-Betriebssystemen auch Apple Mac OS X, CentOS Linux, HP-UX, IBM AIX, SUSE Linux, Oracle und Red Hat Enterprise Linux sowie Sun Solaris.

Analog dazu ist die Unterstützung nicht nur auf Softwareprodukte von Microsoft beschränkt, sondern umfasst auch weit verbreitete Programme wie Adobe Reader, Flash Player, Shockwave und AIR, Sun Java, Winzip, Macromedia Flash Player, Firefox, Novell Clients, Quicktime Player, VMware Player, Server und Workstation, Skype und Citrix ICA Client. Dabei übernimmt das Tool nicht nur das Patchen von Schwachstellen, sondern kümmert sich auf Wunsch auch um die Neuinstallation der genannten Programme. Mit dem Zusatz "Content Wizard" kann der Administrator ergänzend eigene Softwarepakete zur (De)-Installation schnüren und auf diese Weise Patch and Remediation zur individuellen Softwareverteilung nutzen.

Installation nach Maß

Um erste Erfahrungen mit Patch and Remediation zu sammeln, bietet Lumension drei Trial-Varianten an. Bei "Easy Track" kann der Administrator sich die Funktionsweise remote in einer virtuellen Umgebung ansehen, die der Hersteller auf eigenen Servern hostet. "Fast Track" beinhaltet den Download einer vorbereiteten virtuellen Maschine für den VMware Player. Dies hat den Vorteil, dass ein Test in Verbindung mit eigenen Clients in einer eigenen Umgebung möglich ist, ohne dass umfangreiche Vorbereitungen notwendig sind. Die Variante "Total Track" letztendlich erfordert eine komplette Installation auf einem eigenen Server, wobei ein Mitarbeiter von Lumension unterstützend zur Seite steht. Für unseren Test entschieden wir uns für die Variante Fast Track, wozu uns der Hersteller mit einer aktuellen Installation mit längerer Laufzeit als den sonst üblichen 15 Tagen versorgte. Die virtuelle Maschine war mit 2 GByte RAM sowie zwei CPUs konfiguriert und dürfte damit auf jeglicher aktueller Dual-Core-Hardware problemlos laufen. Im Test funktionierte die Umgebung reibungslos, nur erweiterten wir die Platte, um in größerem Umfang Patches herunterladen zu können.

Als erfreulich einfach erwiesen sich im Test die Arbeiten zur Inbetriebnahme.

Systemvoraussetzungen

Der Patch and Remediation Server läuft unter Windows 2003 / 2008 (R2) Server und setzt zwingend eine englische Betriebssysteminstallation voraus. Als Datenbank kommt MS SQL Server 2005 / 2008 zum Einsatz, entweder installiert auf dem Patchserver oder auf einem dedizierten Datenbank-Server. Existiert noch keine Datenbank, richtet das Setup einen SQL Server 2008 Express Edition SP1 mit ein. Hardwareseitig sollte ein aktueller Dual-Prozessor vorhanden sein. Wichtig ist ausreichend Speicherplatz für heruntergeladene Patches. Der Hersteller empfiehlt hier mindestens 32 GByte.

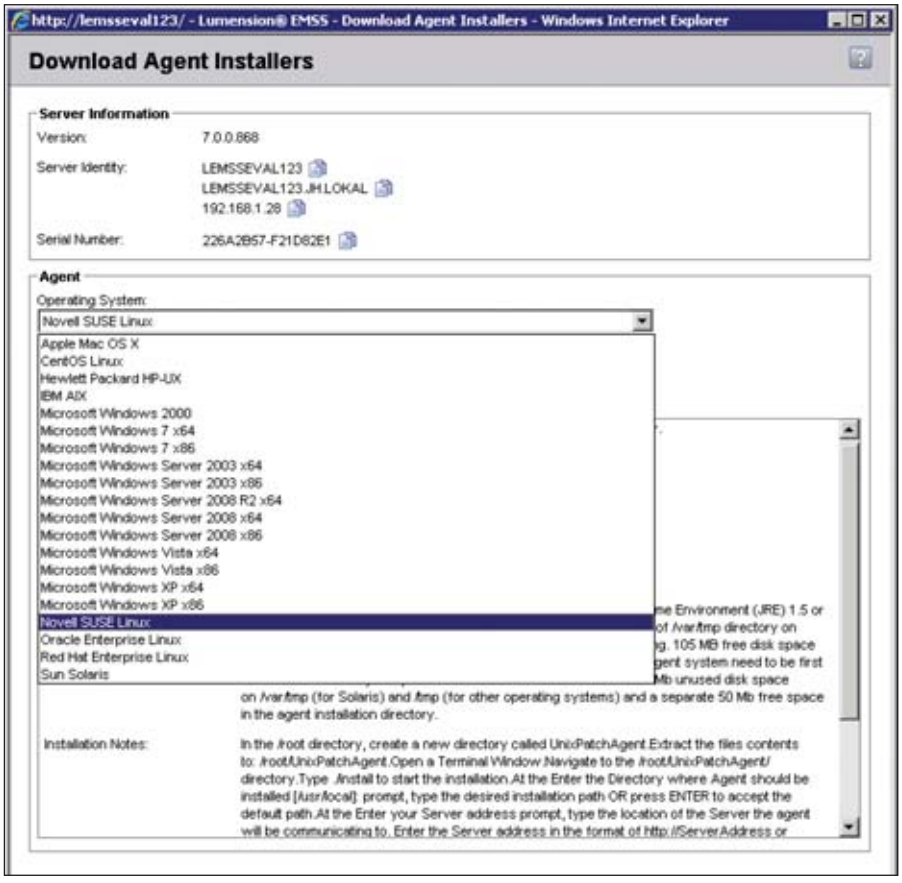


Bild 1: LEMSS unterstützt eine Vielzahl an Betriebssystemen auf den Endsystemen – auch diverse Linux-Derivate

Diese umfassten das Einrichten von E-Mailbenachrichtigungen per SMTP, das Anlegen von Jobs zum Durchsuchen des Netzwerks nach neuen Geräten und das Herunterladen beziehungsweise Installieren von Agenten auf den Clients. Außerdem war für den Betrieb in einer nichtenglischsprachigen Umgebung eine entsprechende Anpassung vorzunehmen, damit, wie von uns benötigt, deutsche Patches heruntergeladen wurden. Bezüglich der Mailbenachrichtigung fiel uns positiv auf, dass sich verschiedene Ereignisse (neue Agenten, neue Schwachstellen, Verteil-Fehler, Lizenz-Probleme, zu geringer Plattenplatz) gezielt unterschiedlichen Adressaten zuweisen lassen, wobei Überlappungen möglich sind.

Flexible Clientanbindung

Patch and Remediation besitzt zwei grundlegende Verfahren, um potenzielle Clients im Netz zu finden: die Suche über IP-Adressen und -Adressbereiche sowie die Suche über Namen und Domänenzugehörigkeiten. Der Administrator kann einen Suchauftrag sofort starten oder per integrierten Zeitplaner einmalig sowie wiederkehrend (wahlweise täglich, wöchentlich, monatlich) vorgeben. Der Auftrag umfasst auf Wunsch mehrere Suchoptionen wie ICMP, Port Scan (FTP, Telnet, SSH, SMTP und http), SNMP, Auflösung von DNS, NetBIOS-Name und MAC-Adresse sowie die Auflösung der Windows-Version. Um gefundene Geräte besser analysieren und beispielsweise das Betriebssystem ermitteln zu können, kann der Administrator dem Suchauftrag Anmeldeinformationen für Windows und POSIX (alle Unix-basierten OS) inklusive Private Key sowie einen SNMP Community String mitgeben. Für die Erkennung von Windows-Clients unter Vista, Windows 7 und Server 2008 ist es sehr wichtig, dass auf diesen Systemen die Netzwerkerkennung und die Dateifreigabe aktiviert sind.

Patch and Remediation nutzt für die Kommunikation mit den Clients einen Agenten. Dieser ist recht schlank gehalten und macht sich am Client überhaupt nicht bemerkbar, auch nicht durch ein Icon in der Taskleiste. Der Anwender kann allenfalls im Taskmanager sehen, dass ein entsprechender Dienst läuft. Eine Deinstallation durch den Anwender ist nicht so einfach möglich, da diese standardmäßig eines Passworts bedarf, das nur die LEMSS-Administrationskonsole verrät. Hierzu ist anzumerken, dass der Administrator das Verhalten eines Agenten per Policy festlegen kann. Diese gibt unter anderem vor, wie der Uninstall-Schutz aussehen soll, wie umfangreich das Logging gewünscht ist und wie häufig eine Kommunikation zwischen Agent und Server stattfinden soll (Heartbeat-Intervall und Antwortzeiten). Neben einer globalen Regel, die vorbelegt mit der Installation kommt, kann der Administrator weitere Regeln definieren und mit den Clients verknüpfen.

Für das Ausbringen der Agenten auf die Clients sieht Patch and Remediation je nach Zielbetriebssystem ein oder zwei Möglichkeiten vor. So kann der Administrator alle verfügbaren Agenten über die Administrationskonsole von LEMSS herunterladen und speichern. Für Windows-Clients ist dies eine MSI-Datei, bei den übrigen Betriebssystemen handelt es sich um einen Java-basierten Agenten als TAR-File. Der Installationsweg an sich obliegt dann dem Administrator (manuell, per (Login)-Script, per GPO oder mittels einer bereits vorhandenen Softwareverteilung).

Bei Windows-Clients ist neben der Installation über eine Datei auch eine Verteilung direkt aus der Konsole heraus per RPC möglich, was letztendlich der komfortabelste Weg ist. Als wir einige Agenten aus der heruntergeladenen MSI-Datei installieren wollten, fiel uns auf, dass LEMSS diese Datei nicht vorher auf die Serverinstallation anpasst, was durchaus möglich wäre. Folglich wurden wir nach der IP-Adresse des Patch-

servers gefragt. Selbstverständlich lässt sich die Installation trotzdem durch eine entsprechende Kommandozeileneingabe automatisieren, in der die IP-Adresse als Parameter mitgegeben wird. Vorteilhaft ist, dass ein Client, auf dem der Agent auf diese Weise installiert wurde, nicht erst noch im Netz gesucht werden muss. Vielmehr kontaktiert er selbst den Server und erscheint dann automatisch in der Clientübersicht.

Patch and Remediation erzeugt aufgrund der aktiven Clients anhand diverser Kriterien wie Betriebssystem und IP-Adresse dynamische Gruppen und weist diesen die Clients zu. So wurden im Test automatisch 22 Gruppen angelegt. Damit ist es beispielsweise ein Leichtes, sich alle Agenten in einem Netzsegment auflisten zu lassen oder eine Aufstellung nach Betriebssystem abzufragen. Neben den dynamischen Gruppen kann der Administrator auch eigene mit beliebigen Filterkriterien anlegen, beispielsweise für eine Gruppierung anhand von Namen oder für die Definition von Patch-Piloten. Um ausgeschaltete Clients zeitnah mit Patches zu versorgen und für diesen Zweck einzuschalten, verfügt Patch and Remediation über eine Wake-On-LAN-Funktion.

Intuitiv bedienbare Konsole

Die LEMSS-Administrationskonsole ist Browser-basiert und lässt sich somit von jedem Client im Netzwerk aufrufen. Ein umfassendes Rollen- und Benutzermanagement, auf das wir noch eingehen werden, sorgt dafür, dass nur berechtigte Anwender mit der Konsole arbeiten können.

Dashboard mit Live-Feed

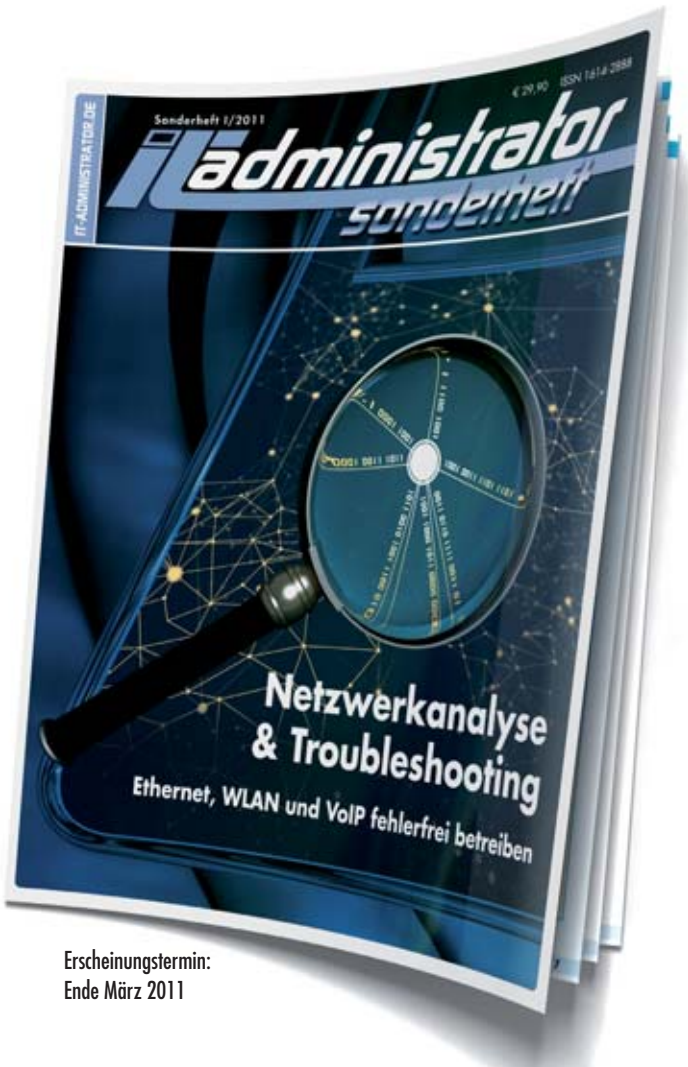
Beim Aufruf der Konsole erscheint auf der Startseite das so genannte Dashboard, das einen ersten Überblick über den Agenten-Patchstatus liefert. So kann der Administrator auf einen Blick ablesen, welche Agenten nicht online sind, auf wie vielen Endsystemen Patches fehlen und wo Schwachstellen existieren. Weiterhin kann er unter anderem den letzten Scan der Agenten abfragen oder nach unvollständigen Verteilungen forschen. Ein Fenster liefert einen Feed von Lumension mit den letzten Neuigkeiten zu veröffentlichten Patches sowie zum Produkt selbst. Letztendlich hat der Administrator die Wahl zwischen insgesamt 18 Fenstern, die in bis zu drei Spalten nebeneinander sowie untereinander angeordnet werden. In der Praxis lassen sich, natürlich etwas abhängig von der Monitorauflösung, etwa neun Ansichten gleichzeitig darstellen, ohne scrollen zu müssen. Als sehr intuitiv empfanden wir die Bedienung dahingehend, dass der Administrator nur eines der Fenster auf dem Dashboard anklicken muss, um sofort zu der entsprechenden Ansicht genauere Informationen in Listenform zu erhalten, beispielsweise, welche kritischen oder empfohlenen Patches fehlen.

Die Funktionen der Konsole sind ebenfalls sehr übersichtlich in fünf Rubriken (Discover, Review, Manage, Reports und Tools) gegliedert. Unter "Discover" sind die bereits oben erwähnten Funktionen zur Agentensuche zusammengefasst. Über die Rubrik "Review" erhält der Administrator Auswertungen in Listenform über Schwachstellen, Pakete und Policies, aber auch über gelaufene Scan- und Verteiljobs. Dabei kann er über das Pull-Down-Menü unter Review grob die Rubrik vorwählen und dann feiner filtern, um beispielsweise eine Übersicht zu erhalten, welche Patches, die im Namen mit "MS10" beginnen, als kritisch eingestuft sind, seitens Lumension aktiv (enabled) sind und auf mindestens einem der überwachten Clients fehlen. Zusätzlich ist eine Filterung über die Gruppierung möglich. Im Laufe des Tests haben wir den Eindruck gewonnen, dass die Anwendung der Filter zwar etwas Erfahrung bedarf, aber letztendlich sehr effektiv und vielseitig ist und es dem Administrator ermöglicht, trotz der Vielzahl der verwalteten Patches genau das herauszufiltern, was ihn jeweils interessiert. Patch and Remediation ist so aufgebaut, dass in der Rubrik Review die Darstellung immer aus Sicht der Softwarepakete erfolgt, auch wenn darüber hinaus eine Filterung der Ansichten anhand der Clientgruppierung möglich ist.

Alle Clients im Blick

Die Betrachtung aus Client- beziehungsweise Agentensicht erfolgt in der Rubrik "Manage". Hier kann sich der Administrator die Clients mit Status (unter anderem online, offline, idle und working) sowie nach

Bild 2: Das Dashboard der LEMSS liefert einen umfassenden, schnellen Überblick und unterstützt eine intuitive Bedienung, indem der Administrator auf den Bereich klickt, der ihn interessiert



Erscheinungstermin:
Ende März 2011

Bestellen Sie jetzt

das IT-Administrator

Sonderheft I/2011!

180 Seiten Praxis-Know-how rund um das Thema

Netzwerkanalyse & Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft I/2011 für € 24,90. Nichtabonnenten zahlen € 29,90. IT-Administrator All-Inclusive Abonnenten "zahlen" für Sonderhefte nur € 19,90 - diese sind im Abonnement dann automatisch enthalten. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.*

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

---

administrator
Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft I/2011 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft I/2011 zum Preis von **€ 29,90** inkl. Versand und 7% MwSt.

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____ Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0211

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

Gruppen oder entsprechend der durchgeführten Agenteninstallationsjobs auflisten lassen. Letzteres liefert die Information, welche Agenten wann installiert wurden. Nachdem LEMSS nicht nur eine Schwachstellenanalyse betreibt, sondern zusätzlich eine Hardwareinventarisierung durchführt, kann der Administrator sowohl die Hardware eines Endpunkts abfragen als auch Analysen durchführen, welches System mit welcher Hardwarekomponente bestückt ist (unter anderem RAM-Ausstattung, BIOS-Typ, Architektur). Zudem liefert Patch and Remediation hier Informationen über die durchgeführten Verteilungen.

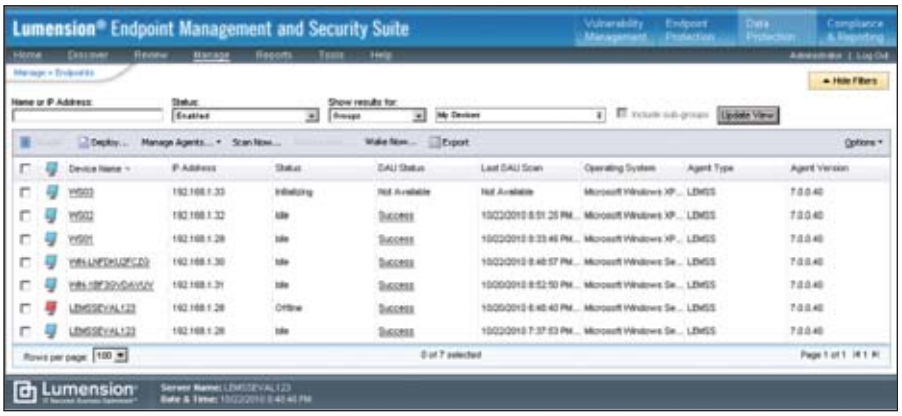


Bild 3: Auf einen Blick kann sich der Administrator den Clientstatus anzeigen lassen und bei Bedarf filtern

Klickt der Administrator in einer der Ansichten der Manage-Rubrik auf einen Client, so erhält er wirklich umfassende Informationen hinsichtlich Inventar, Verteilungen, Schwachstellen sowie globale Informationen wie die Gruppenzugehörigkeiten und die aktuell wirkenden Policy-Vorgaben. Auf Wunsch kann der Administrator einen Endpunkt unabhängig von den regelmäßigen Jobs sofort neu scannen lassen oder diesen durchstarten.

Bezüglich der Verwaltung der Patches lädt LEMSS die verfügbaren Quelldateien standardmäßig nicht sofort herunter, sondern pflegt erst einmal nur die Informationen in die Datenbank ein. Erst wenn die Verteilung eines Pakets erstmals in Auftrag gegeben wird, führt LEMSS den Download durch und speichert die Dateien in einem eigenen Cache auf dem Server. Die Standardeinstellung bewirkt letztendlich, dass nur Pakete heruntergeladen werden, die wirklich benötigt werden, allerdings auch erst zum Zeitpunkt des Verteil-Auftrags, so dass der gesamte Job etwas länger dauert. Um diese Prozesse zu entkoppeln, kann der Administrator optional einen Download beauftragen, ohne diesen mit einer Verteilung zu verknüpfen. Zusätzlich gibt es eine fest einstellbare Option, dass neue, kritische Patches grundsätzlich automatisch heruntergeladen werden, was unserer Meinung nach sehr sinnvoll ist, da diese in der Regel bereits kurz nach der Verfügbarkeit wichtig sind. Ergänzend kann der Administrator hier die Sprachen für herunterzuladende Patches vorgeben, als Standard ist nur Englisch markiert.

Verteilung genau steuerbar

Um im Detail zu untersuchen, wie die Paketverteilung klappt, haben wir neben dem Patchserver mehrere Clients unter Windows XP, 2003 Server sowie 2008 (R2) Server vorbereitet, die nach unserer Installation allesamt bewusst einen sehr lückenhaften Patchstand aufwiesen. Nun wollten wir sowohl nur einen als auch mehrere Clients gleichzeitig patchen. Zudem wollten wir auf einem Teil nur alle kritischen Patches ausrollen, auf einem anderen die kritischen und die empfohlenen. Dies klappte in allen Fällen reibungslos. Besonders gefiel uns, dass es beispielsweise möglich ist, sich anfangs nur einen Endpunkt herauszugreifen, den Verteiljob dann aber auf mehrere Geräte zu übertragen. Sobald der Administrator von einem Client kommend in den Verteil-Assistenten einsteigt, listet Patch and Remediation alle Betriebssystemgruppen mit Anzahl der zugeordneten und ausgewählten Endpunkte auf. So sieht der Administrator sofort, welche anderen Rechner noch in ähnlicher Weise betroffen sind, selbst wenn er sich anfangs nur auf einen Client konzentriert hat. Er hat dann die Möglichkeit, die Auswahl nochmals anzupassen und weitere Clients nach Betriebssystem oder nach Gruppenzugehörigkeit geordnet hinzuzuwählen.

Anschließend erlaubt der Assistent, den Umfang der zu installierenden Pakete nochmals anzupassen. Auf einer weiteren Seite sind dann der Zeitpunkt und die Verteilart (parallel oder sequentiell) festzulegen. Bei einer gleichzeitigen Verteilung lässt sich vorgeben, wie viele Systeme parallel bestückt werden dürfen. Sinnvoll erschien uns ferner die Möglichkeit, dass Patch and Remediation auf Wunsch eine Verteilung aussetzt, sobald diese für einen oder mehrere Endpunkte fehlschlägt. Es ist zwar immer zu empfehlen, eine Verteilung erst auf einigen Pilotsystemen zu erproben, aber diese Option stellt noch eine zusätzliche Sicherheit dar, um bei einem Problem zu stoppen. Allerdings ist zu beachten, dass mit dieser Option ein Patch immer nur auf einem Endpunkt gleichzeitig installiert wird (sequentielle Verteilart), wodurch die Verteilung dann deutlich länger dauert. Leider kann der Administrator nicht vorgeben, dass die Verteilung bis zu einem Stopp auf einer definierten Anzahl an Clients fehlschlagen muss. So besteht die Gefahr, dass der Prozess aufgrund eines einmaligen Fehlers stoppt und gar kein grundsätzliches Problem vorliegt.

In einem nächsten Fenster hat der Administrator die Möglichkeit, für jeden Patch das Verhalten (unter anderem Neustart, Benutzerabfragen, Pakete verketten) vorzugeben. Außerdem sieht der Administrator hier, an welcher Stelle gegebenen-

falls Reboots erfolgen. Im vorletzten Optionsfenster sind die Benachrichtigungen für die Anwender sowohl für die Verteilung als auch für anstehende Neustarts auszuwählen. Ja nach Einstellung bekommt der Anwender einen entsprechenden Info-Text eingeblendet und kann dann die Verteilung oder den Neustart abbrechen oder aussetzen. Damit hat er die Möglichkeit, seine Arbeit erst sinnvoll beenden zu können. Das letzte Fenster beinhaltet dann eine Übersicht aller gewählten Einstellungen zur Kontrolle.

Im Test haben wir verschiedene Jobs durchführen lassen, wobei uns die Vielfalt der Optionen und die dadurch gegebene Flexibilität überzeugt hat. Allerdings bedeutet die Vielzahl der möglichen Optionen auch, dass es erforderlich ist, Jobs mit Sorgfalt zu beauftragen, um alle Angaben korrekt vorzugeben. Dies ist sehr wichtig, da Patch and Remediation wie bereits eingangs erwähnt nicht nur das Patchen bereits installierter Software übernimmt, sondern auch die Neuinstallation der am Anfang des Artikels aufgelisteten Produkte. Wer also beispielsweise einen Auftrag absetzt, der pauschal alles installieren soll, was nicht gepatcht ist, wird anschließend diverse Neuinstallationen wie Adobe Reader, Mozilla Firefox, Quicktime Player und so weiter auf den Clients vorfinden. Hier ist also besondere Vorsicht geboten. Verwirrt hat uns besonders die von uns gewählte Filteroption "Not Patched", die letztendlich keinen Einfluss darauf hatte, dass auch Pakete für Neuinstallationen ausgewählt wurden.

Gutes Rollenmanagement und Reporting

Über ein erfreulich detailliertes Benutzer- und Rollenmanagement lassen sich die Zugriffsrechte bei der Arbeit mit Patch and Remediation recht genau einteilen. Standardmäßig sind vier Rollen (Administrator, Gast, Manager und Operator) vordefiniert. Eine Rolle setzt sich zusammen aus einer Vielzahl an Rechten innerhalb der Suite, weiterhin lässt sich genau vorgeben, auf welche Gruppen und/oder Endpunkte eine Rolle ein Recht hat. Somit ist es durchaus denkbar, dass bei der Verwendung in einer großen heterogenen Umgebung, wo es womöglich getrennte Administratorenteams für die Windows- und Linux-Systeme gibt, jedes Team nur die jeweils zugewiesenen Endpunkte betreuen kann.

Hinsichtlich der Benutzer arbeitet Patch and Remediation sowohl mit lokalen als auch mit Domänenbenutzern. Letztere lassen sich problemlos hinzufügen und auch mehrere in ein Fenster eintragen. Die Routine sucht die angegebenen Benutzer im Active Directory und führt dabei gleich eine Existenzprüfung durch. Gefundenen Benutzern kann der Administrator eine der vorhandenen Rollen zuweisen. Sollen alle Benutzer die gleiche Rolle bekommen, ist dies mit einer Vorauswahl möglich.

Sehr umfangreich ist das in Patch and Remediation integrierte Reporting. Insgesamt 35 Berichte sind komplett vorbereitet. Die Darstellung erfolgt entweder gegliedert in acht Rubriken (Konfiguration, Verteilung, Inventarisierung, Status, Regeln, Power Management, Risiken, Schwachstellen) oder als lange Liste. Über entsprechende weitere Parameter ergeben sich letztendlich weitaus mehr Auswertungen, die abgefragt werden können. So lassen sich einzelne Reports nach Verteilungen, Paketen, Geräten oder Gruppen erstellen. Das Ergebnis erfolgt teilweise als PDF-Datei und teilweise als HTML-Ausgabe. Die Erstellung eigener Reports über die bereits vordefinierten hinaus ist allerdings nicht vorgesehen.

Eigene Inhalte erstellen

Als kostenpflichtige Option zu Patch and Remediation bietet Lumension den "Content Wizard" an. Dieser Zusatz erweitert das Basiswerkzeug dahingehend, dass der Administrator Policies für ein individuelles Powermanagement sowie zur Einhaltung von Sicherheitsvorgaben definieren kann. Der Content Wizard erlaubt zudem die Erstellung beliebiger eigener Tasks. Ein Administrator kann außerdem eigene Pakete zur Softwareverteilung sowie zur Deinstallation erstellen und Definitionen anlegen, um eigene Clientinhalte zu erkennen, zu verteilen und auszuwerten.

Hinsichtlich des Power Managements lassen sich beispielsweise Regeln vorgeben, nach welcher Inaktivitätszeit Clients in den Standby- oder Schlafmodus versetzt werden sollen. Die Regeln werden über die Agenten und damit unabhängig von GPOs durchgesetzt. Ein Vorteil ergibt sich damit vor allem in heterogenen Umgebungen, da die Definitionen dank der Agenten Betriebssystem-unabhängig wirken.

Über den Content Wizard hat der Administrator Zugriff auf alle von Lumension gelieferten Pakete. Das ist insofern recht

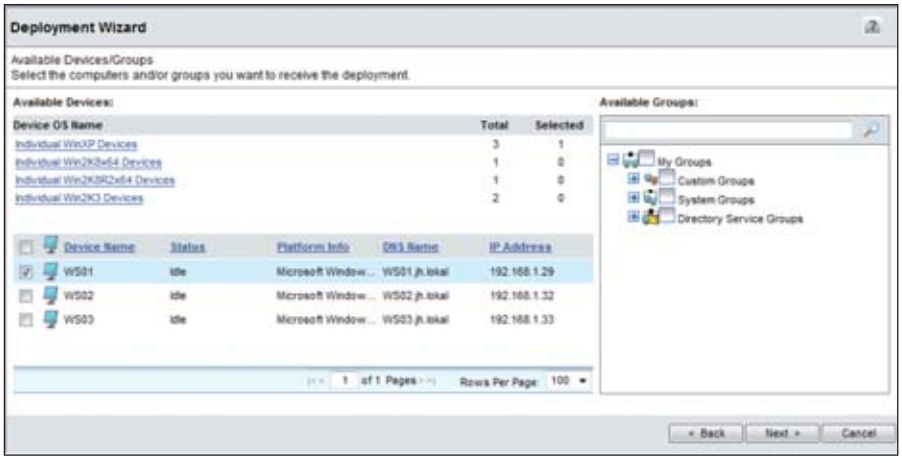


Bild 4: Bei der Definition eines Verteiljobs hat der Administrator die Möglichkeit, ausgehend von einem Endgerät im Verlauf noch weitere hinzuzufügen

hilfreich, da sich der prinzipielle Aufbau so schneller erschließt. Die Erstellung eigener Pakete ist aber dennoch eine komplexe Angelegenheit, die in der Regel ein Scripting erfordert, um die Voraussetzungen und Abhängigkeiten zu prüfen und die eigentliche Aktion durchzuführen. Einfacher gestalten sich die Policy-Erstellung sowie das Einrichten von Power-Management-Regeln.

Eine weitere Option der LEMSS, die die Funktionalität über das Patchen hinaus noch erweitert, ist das Modul "Security Configuration Management", um sicherheitsrelevante Fehlkonfigurationen wie beispielsweise zu kurze Passworte zu erkennen. Das NAC-Modul bietet die Möglichkeit, einer beliebigen NAC/NAP-Lösung Informationen über den Compliance-Status eines Rechners zu übergeben (beispielsweise, dass ein zwingend vorgeschriebener Patch fehlt). In Verbindung mit einer NAC/NAP-Lösung kann dann ein solcher Rechner in ein Quarantäne-Netz verschoben werden, bis seine zwingend notwendigen Patches (Mandatory Baselines) angewendet sind. Während sich Power Management-Richtlinien bereits mit dem Content Wizard einrichten lassen, wird das Reporting als eigenes Modul bepreist. Kostenfrei sind die Addons Wake-On-Lan und Remote Systems Management.

Fazit

Patch and Remediation beschränkt sich nicht nur auf das Patch-Management von Windows-basierenden Clients und auf Microsoft-Produkte, sondern unterstützt zudem verschiedene Linux- und Unix-Betriebssysteme. Dadurch eignet sich das Werkzeug gut für den Einsatz in heterogenen Umgebungen und großen Netzwerken. Unterstützt wird weiterhin das Management verbreiteter Softwareprodukte, wobei es hier nicht nur um das Patchen von Schwachstellen geht. Vielmehr fungiert Patch and Remediation dann auch als Werkzeug zur Softwareverteilung und führt auf Wunsch Neuinstallationen durch. Gefallen hat uns die erfreulich intuitive Bedienung der Konsole. Dadurch gelingt es, trotz der vielen verwalteten Pakete immer noch den Überblick zu behalten und die Agenten gezielt zu betreuen. Etwas Vorsicht ist beim Erstellen von Patch-Aufträgen geboten, damit nicht im gleichen Zug unbeabsichtigt Neuinstallationen durchgeführt werden.

Durch zusätzliche Optionen wie Power Management und Security Configuration Management sowie ein NAC-Modul lässt sich der Funktionsumfang der Suite sinnvoll erweitern. In der Vorbereitung sind Module zur Überwachung der verwendeten Applikationen, zur Kontrolle der genutzten Wechseldatenträger sowie zur Virenabwehr. Letztendlich aber versteht sich diese Suite nicht als Werkzeug für eine vollständige Client-Rundumpflege mit Helpdesk, Lizenzüberwachung und Profilverwaltung, sondern fokussiert in erster Linie auf die Bereiche Compliance, Sicherheit und Risikomanagement. *(ln)*

Produkt
Software zum Betriebssystem-übergreifenden Patchmanagement.

Hersteller
Lumension
www.lumension.com

Preis
Der Basispreis für die LEMSS-Plattform liegt bei 1.546 Euro, hinzu kommt die jährliche Subskription von rund 14 Euro pro Agenten. Die jährlichen Kosten für den optionalen Content Wizard, das Security Configuration Management und das Power Management liegen jeweils bei knapp 5 Euro pro Endsystem. Die angegebenen Preise gelten für Windows-Clients.

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

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

Patch-Management	8
Reporting	9
OS-Unterstützung	8
Installation und Bedienung	8
Dokumentation	7

Dieses Produkt eignet sich

optimal für größere, heterogene Umgebungen, in denen nicht nur Windows-Clients und Microsoft-Produkte gepatcht werden sollen. Dann kann das Tool hinsichtlich Einsatzbreite alle seine Stärken voll zur Geltung bringen.

bedingt für größere und mittlere, eher homogene Umgebungen, wo der Fokus auf dem Patchen von Microsoft-Produkten liegt. In diesem Fall kommt Microsoft WSUS als kostenlose, wenn auch nicht ganz so komfortable Alternative durchaus in Frage.

nicht für kleinere Umgebungen mit Windows-Clients und MS-Produkten. Gegenüber dem kostenlosen WSUS dürften sich Investition und Mehrwert unseres Erachtens nicht rechnen.

Lumension Patch and Remediation 7.0

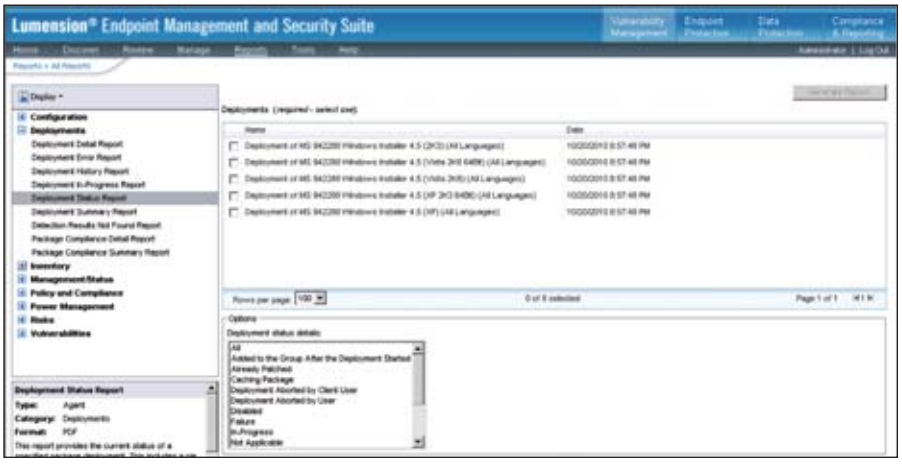


Bild 5: Eine Vielzahl an Berichten ist bereits vorbereitet, die Auflistung erfolgt auf Wunsch thematisch gegliedert

Einkaufsführer: Hybrides Backup lokal und in der Cloud

Mit Bodenhaftung in die Wolke

von Sandra Adelberger

Neben lokal implementierten Disaster-Recovery-Lösungen für physikalische und virtuelle Umgebungen rücken zunehmend Services für die Image-basierte Sicherung in der Cloud ins Blickfeld, die vor allem für kleine und mittlere Unternehmen mit begrenzten IT-Budgets attraktiv werden. Dabei gilt es, sowohl für die Implementierung einer Online-Backup-Lösung als auch auf der lokalen Seite wichtige Punkte zu beachten, damit die drei Ebenen aus physikalischem, virtuellem und Cloud-Backup harmonieren und sich ergänzen. Dieser Einkaufsführer erläutert, was beim Einkauf von Backupkapazitäten in der Cloud zu beachten ist und welche lokalen Voraussetzungen zu schaffen sind.

Neben klassischen Onsite-Backup-Modellen rücken verstärkt auch neue Cloud-Angebote ins Blickfeld. Denn mit der fortschreitenden Entwicklung und Akzeptanz von Cloud-Backup-Services bietet sich gerade für kleine und mittlere Unternehmen eine erschwingliche Möglichkeit, Daten sicher auszulagern, ohne dabei in zusätzliche Storage-Hardware oder Rechenzentren investieren zu müssen. Die Online-Sicherung stellt dabei eine gute Ergänzung zu lokalen Sicherungskonzepten dar, um bei einem Komplettausfall oder physikalischem Schaden der Hardware auf eine externe Sicherung aller Daten und Systeme zugreifen zu können. Die Wiederherstellung einzelner Dateien oder kompletter System-Images erfolgt in diesem Fall aus einer sicheren Cloud-Umgebung.

Und das kommt insbesondere kleinen oder mittelständischen Unternehmen zugute. Denn Status quo im Enterprise-Bereich ist, dass in der Regel kritische Systeme in räumlich getrennte Rechenzentren repliziert werden. Administratoren in kleineren Firmen hingegen stehen solche Möglichkeiten nicht offen. Ihnen bleibt oft nur die Variante, eine aktuelle Bandkopie bei sich zu Hause aufzubewahren.

Dass Online-Backup voll im Trend liegt, prognostizieren auch führende Marktforschungsinstitute. So rechnet Gartner mit einem jährlichen Marktwachstum von 22 Prozent. IDC stellt zudem fest, dass die meisten Unternehmen zu einem Hybridmodell tendieren, mit dem sie die Vorzüge und die Leistungsfähigkeit eines lokalen Backupsystems mit der Flexibilität und der zusätzlichen Sicherheit einer Cloud-Storage-Lösung kombinieren können.

Sicherheitsaspekte bei der Einführung von Cloud-Backup

Bei der Entscheidung für einen Cloud-Backup-Service sollten Unternehmen darauf achten, dass die angebotenen Lösungen insbesondere auch die kritischen Sicherheitsaspekte beim Online-Backup berücksichtigen. Dazu gehören Benutzerauthentifizierung, Verschlüsselung der Backups wie beispielsweise durch AES-256 sowie flexible Aufbewahrungszeiträume.

Ein entscheidender Punkt ist in diesem Zusammenhang auch der Ort des Datencenters. Gemäß einer entsprechenden EU-Richtlinie muss sich das Rechenzentrum zur Nutzung durch europäische Unternehmen innerhalb der EU befinden. Vor allem unter Compliance-Gesichtspunkten sollten vor der Auswahl eines Anbieters klare Antworten auf dem Tisch liegen, zum Beispiel, ob sich die Sicherheitsstandards des Anbieters mit den eigenen decken. Auch Aspekte wie die erforderlichen Wiederherstellungszeiten für einzelne Dateien oder komplette Systeme müssen geklärt werden. Zudem sollte gewährleistet sein, dass der Online-Backup-Service heterogene IT-Infrastrukturen aus virtuellen und physischen Umgebungen unterstützt, wie sie heute in vielen Unternehmen bereits

vorhanden sind. Im Hinblick auf einfache IT-Administration und einen minimalen Verwaltungsaufwand ist die Möglichkeit einer zentralen Verwaltung von lokalen und Online-Backups für physische und virtuelle Maschinen von Vorteil.

Das sollte der Cloud-Dienstleister bieten

Die Ausstattung des Provider-Rechenzentrums selbst spielt ebenfalls eine erhebliche Rolle bei der Sicherheit. Unabdingbar sind hier unter anderem eine redundante, unterbrechungsfreie Stromversorgung, Brandschutztüren, Luftfeuchtigkeitskontrollen und mehrere Sicherheitsstufen bei der Zugangskontrolle. Neben der zusätzlichen Sicherung aller Daten durch ein internes Backup-System ist auch eine 24x7-Netzwerküberwachung im Rechenzentrum unverzichtbar.

Nicht zuletzt sollten bei der Einbindung von Cloud-Backup auch die nötigen Bandbreiten für eine performante Nutzung des Services zur Verfügung stehen. Integrierte Technologien für inkrementelle Backups sowie Datenkompression machen sich in diesem Zusammenhang bezahlt. Ohne Abstriche bei der Sicherheit oder Integrität lassen sich die Datenmengen vor dem Online-Backup dadurch deutlich verringern.

Eine weitere Möglichkeit, große Datenmengen zu übermitteln, bieten beispielsweise inkrementelle Backups. Die initiale Vollsicherung wird dabei verschlüsselt auf einer Festplatte gespeichert und zum Upload an das Rechenzentrum geschickt. Danach sind nur noch inkrementelle Sicherungen erforderlich, die komfortabel über das Internet übertragen werden können. Fällt auf Unternehmensseite ein Server aus, sollte auch problemlos eine Rücksicherung erfolgen.

Bei allen Vorteilen, die eine Cloud-Backup-Lösung bietet, sollten Unternehmen aber eines nicht vergessen: Die lokale Sicherung und Wiederherstellung physikalischer und virtueller Maschinen wird allein schon im Hinblick auf die Geschwindigkeitsvorteile, die das LAN bietet, mittelfristig der Standard im Backup-Umfeld bleiben. Die Einbindung von Cloud-Storage eröffnet Unternehmen allerdings eine neue Flexibilität, indem sie ihre Disaster-Recovery-Lösung durch einen entfernten Speicherort ergänzen und sicherer machen können. Damit werden Hybrid-Modelle aus lokalem und Cloud-Backup in Zukunft verstärkt nachgefragt.

Lokale Backup-Voraussetzungen für physikalische und virtuelle Umgebungen

Für die erfolgreiche Umsetzung eines Hybrid-Konzeptes müssen jedoch auch auf lokaler Ebene die konzeptionellen Voraussetzungen stimmen. Dazu ist vor allem eine Identifizierung unternehmenskritischer Datenbestände unabdingbar. Auch die für die Wiederherstellung der Daten vorgegebene Zeit, die Recovery Time Objective (RTO), spielt in diesem Zusammenhang eine entscheidende Rolle. Fällt beispielsweise der Web-, E-Mail- oder Hauptdatenbank-Server aus, ist es für jedes Unternehmen unerlässlich, dass das System innerhalb von Minuten wieder läuft.

Technisch Verantwortliche in Unternehmen müssen nicht nur definieren, was gesichert werden soll, sondern auch festlegen, wie oft und welche Art von Backup erstellt wird. Die Durchführung einer täglichen Sicherung hat sich über die Jahre bewährt, normalerweise nachts, da dann nur selten auf die Systeme zugegriffen wird. Die heutigen IT-Umgebungen sind jedoch auf längere Betriebszeiten ausgelegt, weshalb dieser Ansatz oft nicht mehr anwendbar ist. Moderne Backup-Lösungen ermöglichen eine zeitlich unabhängige und automatisierte Sicherung im laufenden Betrieb.

Im Allgemeinen sollten Unternehmen bei der Einführung einer Backup-Lösung die Bereiche Shared Resources (gemeinsam genutzte Ressourcen), Arbeitsplatz-

Einsatz und Voraussetzungen für Onsite- und Cloud-Backup

	Onsite-Backup	Cloud-Backup
Physikalische Server	- Imaging-Backup - Inkrementelle/Differentielle Backups - File Backup	- Imaging-Backup - Inkrementelle Backups, Initial seeding - File Backup
Virtuelle Server	Agentenloses / Host-basiertes Backup / VCB / Backup über Agenten	Agentenloses Backup
Datensicherheit	Abhängig vom Vertraulichkeitsgrad der Daten, AES-265-Verschlüsselung	AES-256-Verschlüsselung und Benutzerauthentifizierung
Richtlinien	Jeweilige Compliance-Vorgaben	Jeweilige Compliance-Vorgaben, insbesondere Datencenter innerhalb der EU (bei Nutzung durch europäische Unternehmen)
Recovery Time	Schnell, über LAN	Mittel, Large Scale Recovery
Internet-Bandbreite	Nicht relevant	Je nach Datenaufkommen und Sicherungsmethode (höhere Geschwindigkeit durch Datenkompression und inkrementelle Backups)
Strategischer Ansatz	Lokales Disaster-Recovery-Konzept	Hybrid-Ansatz: Zusätzlicher Sicherheitslevel für lokales Backup
Speichermedien	Lokal angeschlossene Festplatte, NAS, SAN, FTP-Server, Optische Geräte, Band	Für inkrementelle Backups: IDE, ATA, SATA sowie per USB angeschlossene Laufwerke
Kosten	Fixkosten für Infrastruktur, Hardware	Variable Kosten (nutzungsabhängige Preismodelle), keine zusätzlichen Investitionen in Rechenzentren

rechner, Mobile PCs und virtuelle Ressourcen differenziert berücksichtigen. Ein Punkt, der immer wichtiger wird, ist das Backup von virtuellen Desktops, Servern oder Storage-Arrays. Für einen umfassenden Schutz und für die Wiederherstellung einzelner virtueller Maschinen werden meist spezielle, für virtuelle Technologien konzipierte Tools benötigt. Dabei werden zur Absicherung von virtuellen Maschinen in der Praxis unterschiedliche Verfahren genutzt – abhängig von verschiedenen Faktoren wie Zeit, Personalressourcen, Budget oder Verlusttoleranz. Die eingesetzte Backup-Lösung sollte dem technischen Entscheider in jedem Fall genügend Flexibilität bieten und alle gängigen Methoden wie Host- oder Agenten-basiertes Backup unterstützen. Neuere Host-basierte Backup-Lösungen arbeiten direkt auf der Hypervisor-Ebene und ermöglichen so granulare Backup- und Recovery-Optionen, ohne einen Agenten in jeder virtuellen Maschine installieren zu müssen. Disaster-Recovery-Lösungen, die Anwendern genügend Flexibilität für heterogene Umgebungen bieten und eine von der Hardware oder virtuellen Plattform unabhängige Wiederherstellung der physikalischen und virtuellen Maschinen im Netzwerk bieten, sind in der Regel die beste Wahl.

Hinsichtlich der Backup-Medien standen bisher Tape-basierte Lösungen im Vordergrund. Heute werden aber auch Backup-to-Disk (B2D)-Lösungen verstärkt nachgefragt, da sie eine hohe Geschwindigkeit bieten und kostengünstiger geworden sind. Bei der langfristigen Ablage der Daten entscheiden sich viele Unternehmen aber nach wie vor für Magnetbänder, da sie zum einen oft kostengünstiger sind und zum anderen die Auslagerung der Daten an einen anderen Ort erlauben. Bei einer B2D-Lösung müsste hier eine Replikation der Daten erfolgen, was für das Unternehmen den Kauf eines zusätzlichen Arrays bedeuten würde. Genau an diesem Punkt des Speicherortes und -mediums kommt das Thema Cloud-Backup als effiziente und kostengünstige Alternative vermehrt ins Spiel.

Fazit

Cloud-Storage hat inzwischen sein Hype-Image hinter sich gelassen. Die in der Vergangenheit – oft auch zu Recht geäußerten – Sicherheitsfragen werden heute weitgehend berücksichtigt. Cloud-Backup-Lösungen sind inzwischen zu einem ausgereiften und zuverlässigen Service geworden. Und die jetzt verfügbaren Angebote ermöglichen es auch kleinen und mittelständischen Unternehmen, eine Cloud-basierte Sicherung und Wiederherstellung neben der lokalen Datensicherung kostengünstig zu realisieren. *(jp)*

Dipl. Inform. (FH) Sandra Adelberger ist Director Product Management EMEA bei Acronis.

Benutzerauthentifizierung mit PAM

User identifiziere dich

von Thorsten Scherf

Um die Identität eines Benutzers festzustellen, ist eine wie auch immer geartete Authentifizierung notwendig. Dies übernimmt in der Regel nicht die jeweilige Software selbst, sondern ein zentrales und modulares Framework. Für Linux-Umgebungen existiert mit den Pluggable Authentication Modules (PAM) ein modulares Framework, um komplexe Authentifizierungs-Regelsätze zu erstellen. In diesem Workshop erklären wir, was genau bei der Anmeldung über PAM vorgeht und wie Sie dabei auch biometrische Elemente wie einen Fingerabdruck einbinden können.

Quelle: picturia - Fotolia.com

Auf Unix- und Linux-Systemen funktioniert die Benutzeranmeldung üblicherweise über die beiden Dateien */etc/passwd* und */etc/shadow*. Meldet sich ein Benutzer mit Namen und Passwort an einem System an, beispielsweise über *login*, so erzeugt dieses Kommando eine kryptografische Prüfsumme des eingegebenen Benutzerpasswortes und vergleicht das Ergebnis mit der gespeicherten Prüfsumme für diesen Benutzer aus der Datei */etc/shadow*. Stimmen beide überein, so ist der Benutzer korrekt authentifiziert, anderenfalls schlägt die Anmeldung fehl.

In großen Umgebungen findet keine Anmeldung über lokale Dateien statt – stellen Sie sich ein Netzwerk mit Hunderten von Rechnern vor, wo der Vorgang beim Anlegen eines neuen Benutzerkontos auf jedem System wiederholt werden müsste. Aus diesem Grund kommt in großen Umgebungen oftmals ein zentraler Verzeichnis-Server zum Einsatz. Die dezentralen Client-Systeme können diesen Server dann entsprechend abfragen, um die Account-Daten eines Benutzers zu verifizieren. Vor einigen Jahren noch wurde dieser Verzeichnisdienst gerne mit Hilfe des Network-Information-Services (NIS) implementiert, heutzutage kommt jedoch fast ausschließlich das wesentlich sichere und leistungsfähigere LDAP zum Einsatz. Bei der Verwendung eines solchen zentralen Verzeichnis-Dienstes kommt die zu vergleichende Passwort-Prüfsumme also nicht aus der Datei */etc/shadow*. Stattdessen greift die authentifizierende Anwendung auf den zentralen LDAP- oder NIS-Server zurück.

Meldet sich ein Benutzer am System an, muss die Anwendung also in der Lage sein, sowohl die lokalen Dateien als auch den zentralen Netzwerkserver abzufragen. Noch komplizierter wird es, wenn die Authentifizierung des Benutzers über moderne Hardware-Token oder Chipkarten stattfindet – also beispielsweise mit Einmal-Passwörtern oder mit X.509 Zertifikaten. Die Applikation muss hier auf zusätzliche Ressourcen zurückgreifen können, um die Echtheit eines Benutzers zu verifizieren. So etwas statisch im Programmcode zu hinterlegen, ist schwierig und skaliert nicht besonders gut, schließlich wäre für jede neue Art der Authentifizierung eine Änderung des Programmcodes nötig. Geeigneter ist hier ein flexibles Framework, das durch verschiedene Plug-Ins unterschiedliche Authentifizierungs-Verfahren implementiert. Die Applikation selbst ist dann nur noch gegen die entsprechende Bibliothek des Frameworks zu linken und schon stehen der Anwendung sämtliche konfigurierten Verfahren zur Verfügung, um die Authentizität eines Benutzers zu verifizieren.

PAM als Türsteher

Ursprünglich Mitte der neunziger Jahre von Sun Microsystems entwickelt, stehen die Pluggable Authentication Modules (PAM) heutzutage auf den meisten Unix-artigen Systemen zur Verfügung. PAM lagert den kompletten Authentifizierungsvorgang von der eigentlichen Anwendung auf ein zentrales Framework, die PAM-Module, aus. Die Anwendung erhält somit nur noch eine Information zurückgeliefert, ob die Anmeldung des Benutzers erfolgreich war oder nicht. Es ist nun also Aufgabe von PAM, sich darum zu kümmern, einen Benutzer über entsprechende Verfahren zu authentifizieren. Wie diese Verfahren genau aussehen, ist komplett im PAM-

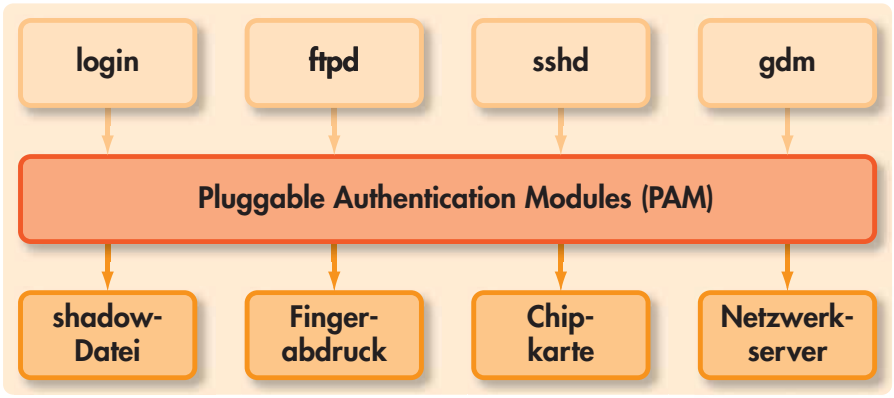


Bild 1: Verschiedene Anwendungen können mittels PAM auf unterschiedliche Verfahren zur Authentifizierung zurückgreifen

Framework hinterlegt, die Anwendung selbst besitzt hierüber überhaupt keine Informationen (siehe Bild 1).

Die Funktionsweise von PAM ist recht simpel. Jede Anwendung, die mit PAM zusammenarbeitet und in diesem Fall gegen die Bibliothek *libpam* gelinkt ist, verfügt im Ordner "/etc/pam.d/" über eine eigene Konfigurationsdatei. Diese hat üblicherweise den selben Namen wie die Anwendung. Beispielsweise also */etc/pam.d/login* für das Login-Programm der Konsole:

```
# ldd `which login`|grep pam
libpam.so.0 => /lib/libpam.so.0
  (0x00290000)
libpam_misc.so.0 =>
  /lib/libpam_misc.so.0 (0x00750000)
```

In dieser Datei unterteilen verschiedene Module die Aufgabenbereiche von PAM. Für jeden Aufgabenbereich steht eine Vielzahl von Bibliotheken zur Verfügung. Je nach Modul haben diese die unterschiedlichsten Aufgaben (siehe Bild 2). Über sogenannte Kontroll-Flags lässt sich das Verhalten von PAM im Fehlerfall regeln, also beispielsweise wenn ein Benutzer ein nicht korrektes Passwort eingegeben hat oder ein X.509 Zertifikat nicht richtig verifiziert werden konnte.

Gliederung der PAM-Konfigurationsdatei

Die in Bild 2 dargestellte PAM-Konfigurationsdatei gliedert sich in vier Abschnitte, jeweils durch ein Modul repräsentiert. Jedes Modul umfasst dabei einen bestimmten Aufgabenbereich.

* auth

In diesem Bereich können Sie sämtliche PAM-Bibliotheken aufrufen, die zur Authentifizierung eines Benutzers dienen. Bei mehreren möglichen Verfahren rufen Sie die einzelnen Bibliotheken einfach hintereinander auf.

* account

PAM-Bibliotheken, die die Autorisierung eines Benutzers durchführen, gehören in diesen Abschnitt. Zur Autorisierung zählt beispielsweise das Überprüfen, ob das eingegebene Benutzer-Passwort momentan eventuell gesperrt ist oder der Benutzer versucht, sich zu einer Zeit am System anzumelden, zu der er sich gar nicht anmelden darf.

* password

Es existieren ebenfalls PAM-Bibliotheken, die zum Umsetzen einer Passwort-Komplexitäts-Policy notwendig sind. Hiermit können Sie dann beispielsweise festlegen, dass das Passwort, welches ein Benutzer setzt, eine bestimmte Anzahl von Sonderzeichen enthalten muss, damit das System es als gültiges Passwort akzeptiert.

* session

Für die Benutzer-Sitzung existiert schließlich noch ein eigener Abschnitt in den PAM-Konfigurationsdateien. Hier können Sie beispielsweise die Dauer einer Benutzer-Sitzung oder die verbrauchten System-Ressourcen loggen, was für das Accounting recht nützlich sein kann. Es lassen sich auch Ressource-Limits erzwingen, beispielsweise wenn es darum geht, wie viel CPU-Zeit ein bestimmter Benutzer in Anspruch nehmen darf oder wie viele Prozesse dieser starten kann.

Kontroll-Flags im Überblick

Direkt neben den Modul-Typen kommen die sogenannten Kontroll-Flags zum Einsatz. Die Aufgabe dieser Flags besteht darin, dem PAM-Framework mitzuteilen, was es als Nächstes tun soll, basierend auf dem Ergebnis, das eine aufgerufene

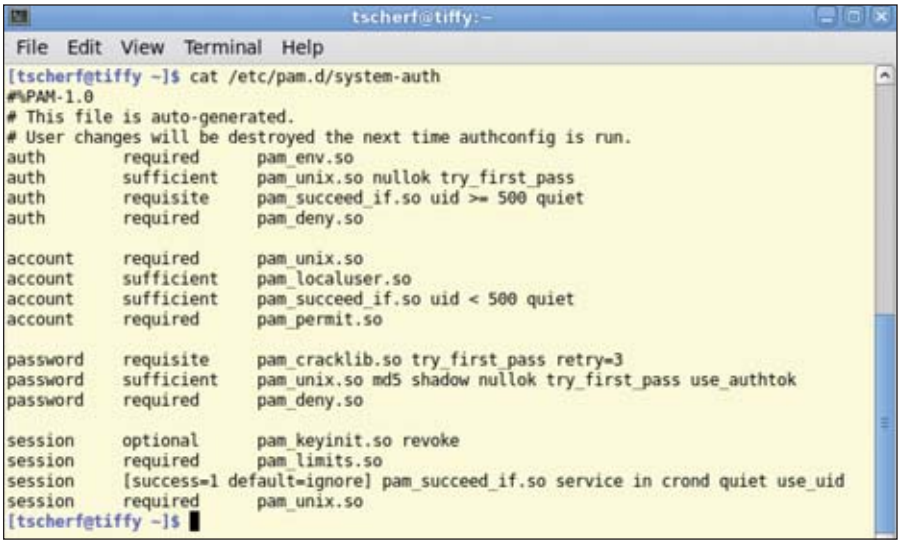


Bild 2: Eine klassische PAM-Konfigurationsdatei gliedert sich in vier Bereiche, in denen unterschiedliche Bibliotheken zur Verfügung stehen

PAM-Bibliothek zurückliefert. Das Ergebnis kann dabei entweder "Erfolg" oder "Fehler" lauten. Es existieren vier vordefinierte Kontroll-Flags:

* required

Liefert eine PAM-Bibliothek einen Fehler zurück, kann PAM einen Benutzer nicht mehr erfolgreich authentifizieren. Allerdings werden noch alle weiteren Bibliotheken des gleichen Modul-Typs ausgeführt, erst dann bekommt der Benutzer eine Rückmeldung darüber, ob die Anmeldung erfolgreich war oder nicht.

* requisite

Verhält sich wie "required", der Unterschied besteht aber darin, dass der Benutzer bei einem Fehler sofort informiert wird.

* sufficient

Einen Fehler ignoriert dieses Flag stillschweigend. Bei einem Erfolg ist der Benutzer direkt erfolgreich authentifiziert, solange alle zuvor aufgerufenen Bibliotheken mit dem Kontroll-Flag "required" ebenfalls einen Erfolg zurückgeliefert haben. Weitere Bibliotheken führt PAM bei einem Erfolg gar nicht mehr aus.

* optional

Hier spielt das zurückgelieferte Ergebnis keine Rolle. Sie können dieses Flag immer dann benutzen, wenn Sie einzelne Bibliotheken aufrufen wollen, wobei deren Ergebnis keine Auswirkungen auf die Benutzeranmeldung haben soll.

Neben diesen vier vordefinierten Kontroll-Flags existieren noch weitere Flags, mit denen Sie sehr fein granuliert auf das Ergebnis der einzelnen PAM-Bibliotheken reagieren können. Weitere Hilfe hierzu finden Sie in der PAM-Dokumentation [1].

Machen Sie sich mit den PAM-Bibliotheken vertraut

Als letztes Element der Konfigurationsdateien sind die eigentlichen PAM-Bibliotheken zu nennen. Diese liegen auf einem 32-Bit-System üblicherweise unterhalb von "/lib/security/", auf einem 64-Bit-System unterhalb von "/lib64/security/". Ein grundlegendes Verständnis dieser Bibliotheken ist wichtig, damit Sie das Framework optimal konfigurieren können. Die wichtigen PAM-Bibliotheken sind in dem unter [2] aufgeführten Dokument beschrieben.

PAM-Anmeldung unter der Lupe

Die in Bild 2 dargestellte PAM-Konfigurationsdatei verfügt im Modul-Abschnitt "auth" über vier Bibliotheken, die das Framework aufruft. "pam_env" sorgt dafür, dass vor dem eigentlichen Login eventuell vorhandene Umgebungsvariablen korrekt gesetzt werden. Diese können Sie in der Datei */etc/security/pam_env.conf* definieren. Ein auf Fedora basierendes System macht hiervon jedoch keinen Gebrauch. Als Nächstes ist mit "pam_unix" die erste Authentifizierungs-Bibliothek aufgeführt. Diese sucht den eigegebenen Benutzernamen in der Datei */etc/passwd* und anschließend das eigegebene Benutzer-Passwort in der Datei */etc/shadow*. Ist sie korrekt, so liefert die Bibliothek ein erfolgreiches Ergebnis zurück und der Benutzer ist authentifiziert. Weitere Bibliotheken kommen wegen des Kontroll-Flags "sufficient" dann gar nicht mehr zur Ausführung.

Bei einem Fehler ist als Nächstes "pam_succeed_if" an der Reihe. Ähnlich wie in der vorherigen Bibliothek kommen hier einige Parameter zum Einsatz. Weitere Bibliotheken werden nur dann ausgeführt, wenn der Benutzer, der sich gerade anmeldet, über eine ID größer 500 verfügt. Die Idee dabei ist, dass PAM System-Konten lediglich auf dem lokalen System sucht, reguläre Benutzer-Konten aber durchaus auch auf einem LDAP-Server oder anderswo liegen können. Diese verfügen üblicherweise über eine ID, die grösser ist als 500. Damit der Zugriff auf den LDAP-Server klappt, ist natürlich eine weitere PAM-Bibliothek im auth-Modul Abschnitt notwendig. Diese lautet "pam_ldap". Ist diese vorhanden, greift PAM auf den konfigurierten LDAP-Server zurück. Wie Sie diesen festlegen, erfahren Sie im nächsten Abschnitt.

Liefert auch diese Bibliothek einen Fehler zurück, so kommt schließlich mit "pam_deny" eine Bibliothek zum Einsatz, die immer einen Fehler zurückliefert. Da das Kontroll-Falg "required" lautet, schlägt die Authentifizierung somit also fehl. Interessant ist nun, dass Sie im auth-Abschnitt durch das Stapeln von einzelnen PAM-Bibliotheken, die für die Authentifizierung zuständig sind, mehrere Methoden hintereinander abarbeiten können, bis der Benutzer letztendlich angemeldet ist – oder eben auch nicht, sollte dieser nicht existieren oder die Anmeldung aus einem anderen Grund fehlschlagen.

Im letzten Abschnitt haben wir bereits die Bibliothek "pam_ldap" angesprochen. Nun fragen Sie sich vielleicht, wie Sie dem PAM-Framework mitteilen, welcher LDAP-Server denn abzufragen ist, nachdem Sie die PAM-Konfigurationsdatei manuell angepasst haben. Die gute Nachricht ist, dass Sie diese Aufgabe recht leicht über ein grafisches Tool erledigen können. Auf einem Fedora-System besteht beispielsweise mittels *system-config-authentication* die Möglichkeit, das PAM-System anzupassen, ohne sämtliche Konfigurationsdateien kennen zu müssen.

Wählen Sie hier als Authentifizierungs-Methode LDAP aus, so können Sie den LDAP-Server mit den vorhandenen Benutzer-Daten eintragen. Neben dem PAM-Framework lässt sich hier ebenfalls der Name-Service-Switch konfigurieren. Dieser ist dafür verantwortlich, Name-Lookups durchzuführen, also beispielsweise die UID eines Benutzer-Accounts abzufragen, während PAM primär für die Authentifizierung des Accounts zuständig ist.

Das auth-Modul der PAM-Konfiguration sieht nach der Auswahl von LDAP dann beispielsweise so aus:

Vorteilspreis für IT-Administrator Abonnenten

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Exchange-Training

Hamburg, 14. April 2011
und München, 24. Mai 2011

Trainings-Partner:

Die Komplexität einer Exchange-Infrastruktur ist äußerst hoch und nur mit solidem Wissen ist der Administrator in der Lage, diese zuverlässig und verfügbar zu betreiben, sowie wichtige Features bereitzustellen, die die Anwender für ihre tägliche Arbeit benötigen.

Daher bietet IT-Administrator ein ganztägiges Exchange-Training in Hamburg und München an, das praxisnahes Know-How zu Hochverfügbarkeit, der Veröffentlichung von Exchange im Internet und Troubleshooting vermittelt.

Themen des Trainings:

Hochverfügbarkeit in Exchange Server 2010
- Design
- Konfiguration und Management

Veröffentlichung von Exchange (2003, 2007, 2010) ins Internet über TMG
- OWA
- Outlook Anywhere
- ActiveSync

Troubleshooting Exchange (2003, 2007, 2010)
- Einführung in Tools zur Fehlerdiagnose
- Performance Monitoring

Referent: Jürgen Haßlauer, infoWAN GmbH

Termin: 14. April 2011
Ort: ExperTeach Training Center Hamburg, Esplanade 6, 20354 Hamburg

Uhrzeit: 10.00 bis ca. 17.30 Uhr

Anmeldeschluss: 7. April 2011

Termin: 24. Mai 2011
Ort: ExperTeach Training Center München, Wredestr. 11, 80335 München

Uhrzeit: 10.00 bis ca. 17.30 Uhr

Anmeldeschluss: 17. Mai 2011

Trainings-Partner:

Teilnahmegebühren:
Für IT-Administrator Abonnenten Euro 95,- (zzgl. 19% MwSt.), für Nicht-Abonnenten Euro 165,- (zzgl. 19% MwSt.).
Die Teilnehmerzahl ist auf 25 begrenzt

Mehr Infos und Anmeldeformulare unter
www.it-administrator.de/workshops/

```
auth required pam_env
auth sufficient pam_unix nullok
  try_first_pass
auth requisite pam_succeed_if uid
  >= 500 quiet
auth sufficient pam_ldap
  use_first_pass
auth required pam_deny
```

Wie Sie sehen, kommt hier nun eine zweite Bibliothek (pam_ldap) zum Einsatz, die die Authentifizierung des Benutzers über den angegebenen LDAP-Server versucht.

Vielleicht möchten Sie Ihre Benutzer-Passwörter jedoch nicht im LDAP, sondern lieber auf einem Kerberos-Server hinterlegen. Mit dem Tool *system-config-authentication* geben Sie in diesem Fall für Account-Daten den LDAP-Server an, für die eigentliche Authentifizierung aber den Kerberos-Server. Die entsprechenden Konfigurationsdateien der einzelnen Subsysteme (LDAP/Kerberos) passt das Tool automatisch an (siehe Bild 3).

Bild 3: NSS und PAM können durchaus unterschiedliche Quellen abfragen

Fingerabdrücke nutzen

Einige PAM-Bibliotheken bieten die Möglichkeit, Benutzer beispielsweise auch über Smartcards oder biometrische Merkmale zu authentifizieren. Aktuelle Notebooks besitzen oftmals einen Fingerabdruck-Leser, mit dessen Hilfe sich Benutzer über ihren digitalen Fingerabdruck am System anmelden können. Hierfür existiert unter [3] eine PAM-Bibliothek mit dem Namen "thinkfinger". Laut Dokumentation arbeitet dieses Modul problemlos mit dem UPEK/SGS Thomson Microelectronics Fingerabdruck-Lesegerät zusammen. Dieser findet sich in den meisten aktuellen Lenovo-Notebooks oder existiert als externes Gerät. Die meisten großen Linux-Distributionen bieten bereits fertige Pakete für diese PAM-Bibliothek an. Über die jeweiligen Paketmanager lässt sich die notwendige Software aus den Repositories installieren. Auf einem Fedora-System gelingt dies beispielsweise mittels *yum install thinkfinger*. Bevor Sie die bestehende PAM-Konfiguration ändern, sollten Sie erst einmal die problemfreie Funktionsweise des Gerätes testen. Hierfür lässt sich mittels *tf-tool -acquire* ein Abdruck eines Fingers einlesen. Im Anschluss können Sie diesen dann mittels *tf-tool -verify* überprüfen. Stimmt der Fingerabdruck nicht überein, so lautet das Ergebnis "Fingerprint does *not* match". Die ersten Versuche können durchaus etwas holprig sein, bevor die Funktionsweise des Gerätes in Fleisch und Blut übergeht. Wer den Finger zu schnell oder zu langsam über das Lesefeld zieht, riskiert eine falsche Erkennung des Abdrucks und steigt mit einer Fehlermeldung aus. Funktioniert das Einlesen des Fingerabdrucks schließlich ohne Probleme, so lässt sich die temporär erzeugte Datei mit dem Testabdruck unterhalb von "/tmp" löschen und für jeden Benutzer eine individuelle Datei mit seinem Fingerabdruck auf dem System erzeugen. Der notwendige Programm-Aufruf hierfür lautet *tf-tool --add-user {Benutzername}*. Der Benutzer muss hierfür dreimal seinen Finger über das Lesefeld ziehen. Wurde jeder Abdruck problemfrei erkannt, so speichert das Tool diesen in einer eigenen Datei unterhalb von "/etc/pam_thinkfinger/".

Korrekte Authentifizierungs-Reihenfolge beachten

Hat soweit alles funktioniert, können Sie anschließend die eigentliche PAM-Konfiguration vornehmen. Möchten Sie nun zuerst versuchen, eine Authentifizierung über den Fingerabdruck-Leser durchzuführen, ist das hierfür notwendige PAM-Modul "pam_thinkfinger" vor "pam_unix" aufzurufen. Damit PAM nach einem erfolgreichen Test des Fingerabdrucks nicht noch einmal nach dem Benutzer-Passwort fragt, ist als Kontroll-Flag "sufficient" anzugeben. Dieses bewirkt ja, dass bei einem erfolgreichen Test PAM keine weiteren Bibliotheken zur Authentifizierung mehr aufruft und einen Erfolg an das aufrufende Programm – hier login – zurückliefert. Sollte die Anmeldung über den Fingerabdruck nicht funktionieren, dann springt, sozusagen als Notlösung, "pam_unix" oder eine andere von Ihnen konfigurierte Bibliothek ein und fragt den Benutzer nach seinem regulären Passwort.

Nun wäre es allerdings recht umständlich, müssten Sie für alle Programme die gewünschten PAM-Bibliotheken in jeder einzelnen PAM-Konfigurationsdatei manuell eintragen. Als Lösung existiert hierfür eine Art zentrale PAM-Konfigurationsdatei. Unter Fedora oder Red Hat heißt diese */etc/pam.d/system-auth*, einige andere Linux-Distributionen verwenden für diese Datei den Namen */etc/pam/common-auth*. Hier können Sie alle gewünschten Bibliotheken zur Authentifizierung von Benutzern eintragen. Über das Kontroll-Flag "include" lässt sich diese Datei dann von allen anderen PAM-Konfigurationsdateien aus einbinden. Somit stehen allen Programmen die PAM-Bibliotheken aus der zentralen Konfigurationsdatei zur Verfügung, ab nun also auch "pam_thinkfinger".

PAM kann noch mehr

Wie bereits erwähnt, existieren neben dem auth-Modul noch weitere Module. Im Abschnitt "account" kümmert sich PAM um die Autorisierung eines Benutzers. Hierfür existieren zwei bekannte Bibliotheken, die auf jedem System zur Verfügung stehen – "pam_time" und "pam_access". Hiermit können Sie fein granuliert festlegen, wer zu welcher Uhrzeit von welchem Netzwerkhost oder Terminal auf das lokale System zugreifen darf. Beide Bibliotheken sind, genau wie "pam_thinkfinger", in der zentralen Konfigurationsdatei */etc/pam.d/system-auth* einzutragen. Da es sich hierbei jedoch um Bibliotheken zur Autorisierung anstatt zur Authentifizierung handelt, tragen Sie diese in das account-Modul ein. Über */etc/security/time.conf* konfigurieren Sie dann entsprechende Zugriffsregeln für "pam_time". Die allgemeine Syntax hierfür lautet: "Dienst; TTYs; User;Zeit". Möchten Sie beispielsweise den Zugang zum SSH-Server in der Nacht verbieten, so lässt sich dies durch einen Eintrag *sshd;*;*;!Al2100-0600* erreichen. Wobei die Abkürzung "Al" für sämtliche Tage der Woche, "Wk" für Arbeitstage von Montag bis Freitag und "Wd" für Samstag und Sonntag steht. Eine genaue Beschreibung der Syntax finden Sie in der Konfigurationsdatei selbst. Im gleichen Modul können Sie die Bibliothek "pam_access" aufrufen. Mit deren Hilfe legen Sie fest, welche Benutzer oder Gruppen sich über welche lokalen Konsolen oder Netzwerkrechner mit dem lokalen System verbinden dürfen. Rufen Sie die Bibliothek über die zentrale PAM-Konfigurationsdatei auf, so gelten die Einschränkungen für alle PAM-Dienste.

Möchten Sie diese lediglich für den SSH-Server aktivieren, so ist der Eintrag entsprechend in der Konfigurationsdatei für den SSH-Server, also */etc/pam.d/sshd*, vorzunehmen. Auch für "pam_access" existiert mit */etc/security/access.conf* eine eigene Konfigurationsdatei. Die Syntax für diese Datei lautet: "Rechte:User/Gruppe:Konsole/ Netzwerkrechner". Um eine Anmeldung aller regulären Benutzer auf dem lokalen SSH-Server zu unterbinden, nehmen Sie folgenden Eintrag in der Datei vor: "-:ALL EXCEPT root: ALL". Möchten Sie schnell alle regulären Benutzer von der Anmeldung an Ihrem System ausschließen, ist dies mit der Bibliothek "pam_nologin" kein Problem. Rufen Sie diese einfach in der gewünschten Konfigurationsdatei auf und erzeugen Sie anschließend eine Datei */etc/nologin*. Außer root wird sich nun bis zum nächsten Reboot oder dem manuellen Entfernen dieser Datei kein Benutzer mehr anmelden können.

Auch das PAM-Modul "password" bietet interessante Konfigurationsmöglichkeiten. Die wohl bekannteste Bibliothek in diesem Abschnitt lautet "pam_cracklib". Sie konfigurieren diese über entsprechende Parameter, die Sie einfach wieder an die Bibliothek anhängen. Der folgende Eintrag bewirkt beispielsweise, dass ein Benutzer bei der Auswahl eines neuen Passwortes mindestens acht Zeichen verwenden muss, wobei mindestens eine Zahl, ein Großbuchstabe und ein Sonderzeichen zu verwenden sind:

```
password required pam_cracklib
  dcredit=-1 ucredit=-1 ocredit=-1
  lcredit=0 minlen=8
```

Schließlich existiert mit dem PAM-Modul "session" ein Bereich, der nicht nur für das Accounting hilfreich ist, sondern Sie können hier mittels "pam_limits" eine Vielzahl von Ressource-Limits für Ihre Benutzer erzwingen. Möchten Sie beispielsweise, dass bestimmte Benutzer nicht mehr als 20 Prozesse auf dem System starten dürfen, so legen Sie hierfür eine entsprechende Regel in der Konfigurationsdatei für diese Bibliothek an. Die Datei lautet */etc/security/limits.conf*:

```
foo     soft    nproc   20
foo     hard    nproc   25
```

Fortan darf der Benutzer "foo" initial nicht mehr als 20 Prozesse starten. Allerdings darf dieser selbstständig (mittels *ulimit*) das Limit auf maximale 25 Prozesse erhöhen. Versucht er, über dieses Hard-Limit zu gehen, erfolgt eine Fehlermeldung.

Fazit

Wie Sie sehen, steht mit PAM ein wirklich sehr mächtiges und leistungsstarkes Framework rund um das Thema Benutzer-Authentifizierung, Autorisierung, Password- und Session-Management zur Verfügung. In diesem Artikel konnten wir nur einige der vielen PAM-Bibliotheken vorstellen, wir raten jedoch jedem interessierten Administrator, sich einmal näher mit dem bereits erwähnten PAM-Administrationshandbuch vertraut zu machen. Vielleicht finden Sie hier ja die Lösung für ein Problem, das Sie schon lange beschäftigt. *(ln)*

Link Codes

[1] PAM-Administrationshandbuch
B1P51

[2] Übersicht über diverse PAM-Bibliotheken
B1P52

[3] Bibliothek "pam_thinkfinger":
B1P53

Wege zum Information Rights Management

Bodyguard für Informationen

von Martin Kuppinger

Das Information Rights Management ist kein neues Thema, spielt aber bisher in der IT-Sicherheit noch eine untergeordnete Rolle. Neue Herausforderungen wie etwa die Cloud-Sicherheit könnten dies aber ändern. Denn allen Unkenrufen zum Trotz ist IRM ein Ansatz, der vieles besser kann als etablierte Lösungen der System- und Netzwerksicherheit. IT-Administrator stellt Ihnen das Konzept vor.

Der Begriff des Information Rights Management – kurz IRM – steht für Lösungen, die sich von klassischer Sicherheit dadurch unterscheiden, dass sie direkt das schützen, was schützenswert ist: die Information. Im Gegensatz zu Firewalls, die versuchen, den Zugang zu einem Netzwerk(-segment) zu kontrollieren, oder zu File Server-Sicherheitsfunktionen, bei denen ein Server und die zu einem bestimmten Zeitpunkt darauf gespeicherten Dateien geschützt werden, sind Informationen bei IRM immer geschützt – unabhängig davon, in welchem Netzwerk sie sich befinden oder auf welchem Server sie gerade abgelegt sind. Die Vorgehensweise dafür ist einfach zu umreißen: Die Informationen werden verschlüsselt und mit Zugriffsberechtigungen versehen. Sie können nur von autorisierten Benutzern entsprechend dieser Zugriffsberechtigungen verwendet werden. Da sie verschlüsselt sind, spielt es zunächst keine Rolle mehr, wo sie sich aktuell befinden. IRM fokussiert auf die Informationssicherheit, nicht auf die Netzwerk- oder Systemsicherheit.

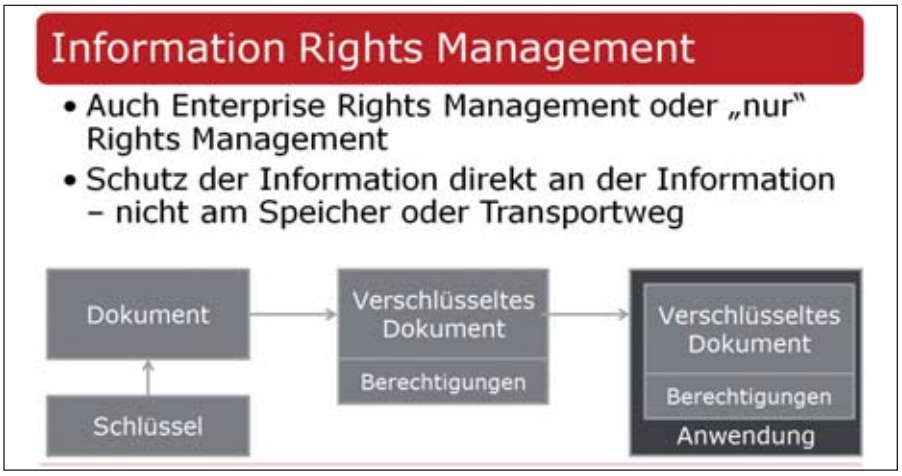


Bild 1: Das Grundkonzept von IRM umfasst den direkten Schutz der Dokumente durch Verschlüsselung

Komplexe Realität

Betrachten wir die Umsetzung von IRM, zeigt sich schnell die Komplexität des Themas. Das beginnt schon bei der Frage danach, welche Informationen überhaupt gesichert werden können. IRM-Lösungen sind auf den Schutz von Dokumenten ausgelegt. Word-Dokumente und andere Office-Dateien, PDF-Dateien, Konstruktionspläne und manchmal auch E-Mails sind Informationstypen, die IRM-Lösungen adressieren. Strukturierte Daten in Datenbanken sind dagegen nicht Gegenstand von IRM-Ansätzen (siehe Kasten "IRM, Datenbanken und PII"). Bei einer Betrachtung der Lösungen verschiedener Anbieter wird zudem deutlich, dass es meist nur eine geringe Zahl unterstützter Anwendungen gibt. Das liegt vor allem daran, dass die Anwendung bei den meisten IRM-Ansätzen sozusagen "IRM ready" sein und den Ansatz des jeweiligen IRM-Anbieters unterstützen muss.

Will ein Benutzer etwa ein geschütztes Dokument öffnen, muss eine Autorisierungsprüfung erfolgen. Darf der Benutzer dieses Dokument überhaupt bearbeiten? Das Dokument muss – eine solche grundsätzliche Autorisierung vorausgesetzt – entschlüsselt werden. Damit ist aber die eigentlich kritische Phase erreicht, da der Schutz nun wegfällt. Aus diesem Grund muss die Anwendung sicherstellen, dass während der Verarbeitung nur solche Aktionen durchgeführt werden, zu denen der aktuelle Benutzer berechtigt ist. Ist in den Berechtigungen beispielsweise definiert, dass er das Dokument nicht ausdrucken darf, muss die entsprechende Funktion im Programm auch deaktiviert sein. Ist zudem festgelegt, dass er keine Teile des Dokuments kopieren darf, muss auch dies verhindert werden. Klar ist aber, dass die Risiken für die Sicherheit von Informationen in dieser Phase am höchsten sind – ein Thema, auf das wir später noch näher eingehen.

Die meisten IRM-Ansätze arbeiten mit Erweiterungen und Schnittstellen in den Produkten, die die Informationen verar-

beiten, also beispielsweise Office-Anwendungen oder CAD-Lösungen. Es gibt aber auch einzelne Ansätze, bei denen der Schutz durch Kontrollmechanismen auf Betriebssystemebene erfolgt. Diese überwachen etwa Dateioperationen, Druckoperationen oder die Nutzung der Windows-Zwischenablage. Dieser Ansatz hat den Vorteil, dass keine Änderungen und Erweiterungen der Anwendungen nötig sind.

Benutzer, Schlüssel, Richtlinien

Nicht nur die Integration in Anwendungen ist komplex, sondern auch das Management von Benutzern, Schlüsseln und den Autorisierungsrichtlinien. Beim Schlüsselmanagement kann das nicht überraschen – Verschlüsselung ist per se eine komplexe Thematik. Das gilt natürlich auch beim IRM, wobei die meisten Lösungen diese Komplexität inzwischen gut verbergen.

Die zweite Herausforderung ist das Benutzermanagement. Informationen sind nicht nur innerhalb des eigenen Unternehmens schützenswert. Gerade wenn Informationen über die Grenzen eines Unternehmens hinaustransportiert werden, geht es um deren zuverlässigen Schutz. IRM muss in der Lage sein, nicht nur mit den internen, beispielsweise im Active Directory verwalteten Benutzern zu arbeiten, sondern über Identity Federation oder Selbstregistrierungsverfahren auch andere Benutzergruppen einbinden können. Nur dann lassen sich die Informationen wirklich über ihren gesamten Lebenszyklus und in allen relevanten Anwendungsfällen schützen.

Hier haben die Hersteller in den vergangenen Jahren deutliche Fortschritte gemacht – Microsoft unterstützt Claims und damit Identity Federation, Adobe setzt auf einfache Selbstregistrierung, um nur zwei Beispiele zu nennen. Schließlich braucht es auch ein einfaches Management von Richtlinien für die Autorisierung. Die Berechtigungen werden im Idealfall automatisch vergeben, um zumindest einen Basisschutz der Informationen sicherzustellen. Allerdings ist dieser oft zu grob, so dass gerade der Informationsersteller auch in der Lage sein sollte, in einfacher Weise Berechtigungen zu definieren – denn der Informationsersteller oder -besitzer weiß in vielen Fällen am besten, für wen ein Dokument eigentlich gedacht ist.

Die Grenzen von IRM

Auch in den Situationen, in denen ein IRM-Konzept konsequent umgesetzt wurde, gibt es Grenzen des Informationsschutzes. Öffnet ein autorisierter Benutzer ein Dokument auf seinem Bildschirm, kann er das auch bei fehlenden Druck- oder Kopierberechtigungen immer noch abfotografieren und diese Information weitergeben – genauso, wie ihm jemand über die Schulter schauen kann. Viel problematischer ist aber, dass es Berechtigungen wie das Kopieren gibt, mit denen Informationen in andere Dokumente übernommen werden können, die nicht unbedingt geschützt sind. Und ausgedruckte Informationen lassen sich natürlich auch wieder einscannen. Auch IRM bietet also keinen absoluten Schutz der Information. Je nach definierten Berechtigungen kann es auch hier zu einem Missbrauch kommen, auch wenn IRM hier deutlich mehr Sicherheit bietet als beispielsweise die Sicherheitsmechanismen von File Servern, bei denen ein Dokument jeden Schutz verliert, sobald es den Server erst einmal verlassen hat.

Die Ansätze der Hersteller

Im Markt der IRM-Lösungen lassen sich zwei Gruppen von Anbietern unterscheiden. Die eine Gruppe setzt auf IRM mit einer Integration auf Anwendungsebene, die zweite Gruppe versucht die Herausforderung auf der Systemebene zu lösen. Zur ersten Gruppe zählen mit Adobe, EMC/Documentum, Microsoft und Oracle die etablierten Anbieter. In der zweiten Gruppe findet sich derzeit als bekannterer Anbieter nur Seclore, ein indischer Softwarehersteller. Außerdem gibt es noch Add-On-Anbieter wie Titus Labs, deren Fokus auf der Unterstützung bei der Klassifizierung von Dokumenten liegt,

um auf dieser Basis automatisch Berechtigungen vergeben zu können, oder SecureIslands, die ebenfalls auf die Klassifizierung als Basis für ein erfolgreiches IRM abzielen. Während Seclore insbesondere mit der Einfachheit seines Ansatzes wirbt, der eben keine komplexe Server-Infrastruktur und kein komplexes Benutzermanagement erfordert, sondern einfach umzusetzen ist, setzen die anderen Anbieter auf unternehmensweite Lösungen oder – insbesondere im Fall von Adobe – auch auf spezialisierte Punktlösungen für spezielle Anwendungsfälle im Informationsmanagement, wie die sichere Verteilung von Rechnungen.

Obwohl vergleichsweise wenige Anbieter im IRM-Markt aktiv sind, liegt hierin dennoch eine der größten Herausforderungen für das Thema: Jeder der Anbieter verfolgt einen etwas anderen Ansatz. Das bedeutet, dass die Integration in Anwendungen wie Microsoft Office, den Adobe Reader oder CAD-Lösungen jeweils in etwas unterschiedlicher Weise bewerkstelligt werden muss. Standards für das IRM, mit denen Anwendungen einfach mit den IRM-Lösungen aller Hersteller zusammenarbeiten könnten, fehlen heute noch. Die Entwicklung solcher Standards, mit denen IRM-Lösungen verschiedener Anbieter gemeinsam eingesetzt werden können und Anwendungsentwickler eine Standardschnittstelle für die Integration von IRM-Funktionalität nutzen können, ist ein kritischer Erfolgsfaktor für IRM.

IRM, Datenbanken und PII

IRM kann nicht alles – insbesondere kann IRM keine strukturierten Informationen in Datenbanken schützen. Das wäre jedoch für den Umgang mit personenbezogenen Daten (PII, personally identifiable information) interessant. Diese Informationen granular mit Zugriffsberechtigungen zu versehen und zu verschlüsseln, würde aber ihre Verwendbarkeit in heutigen Datenbank-Anwendungen verhindern.

Die Problematik ist aber im Grundsatz vergleichbar: Wie lässt sich sicherstellen, dass solche Informationen auch dann geschützt sind, wenn sie erst einmal die gut geschützte Datenbank verlassen haben? Gerade Daten, die in Data Warehouse-Anwendungen landen, aber auch solche, die an andere Anwendungen direkt übergeben werden, befinden sich außerhalb der Kontrolle des ursprünglichen Systems. Es ist allerdings zu befürchten, dass brauchbare Antworten in diesem Bereich noch deutlich länger auf sich warten lassen werden, als es im Bereich der unstrukturierten Informationen der Fall ist.

IRM erhöht Cloud-Sicherheit

Ein Themenfeld, bei dem IRM viele Herausforderungen lösen kann, die sonst kaum zu adressieren sind, ist das Cloud Computing. Eines der größten Risiken dort ist, dass der Administrator eben nicht genau weiß, wo Informationen gespeichert werden. Die Information bewegt sich im Internet gegebenenfalls über verschiedene Server hinweg, ohne dass darüber allzu viel Kontrolle besteht. Umso wichtiger wird es, dass die Information direkt geschützt ist – gerade wenn sich die Systeme selbst nicht absichern lassen, da sie von einem anderen Anbieter betrieben werden (oder sogar einer Kette von Anbietern, weil der Dienstanbieter vielleicht die Amazon EC2 oder eine andere Infrastruktur nutzt, um seinen Dienst überhaupt bereitstellen zu können). IRM schützt die Information direkt, unabhängig davon, wo sie aktuell liegt.

Punktuelle Lösungen vs. flächendeckender Einsatz

Aller Vorteile zum Trotz entwickelt sich der Markt nur langsam. Microsoft liefert die Rights Management Services (RMS) zwar als Standardfunktion der Windows Server aus, genutzt wird die Technologie aber nur in vergleichsweise wenigen Unternehmen. Adobe setzt dagegen in seiner Strategie mehr auf punktuelle Lösungen, die mit anderen Technologien wie dem Rechnungsmanagement eng integriert sind. Und auch Seclore, um ein weiteres Beispiel zu nennen, geht eher opportunistisch in den Markt, wenn beispielsweise bestimmte Dateiübertragungen zwischen verschiedenen Banken gezielt gesichert werden müssen.

Der Adobe-Ansatz hat dabei den Charme, dass es einen konkreten Anwendungsfall gibt, der adressiert wird, was einfacher durchsetzbar ist als ein komplexes Infrastrukturprojekt. Andererseits ist IRM für ein durchgängiges Konzept der Informationssicherheit so wichtig, dass IT-Verantwortliche das Thema auch strategisch als Teil der Sicherheitsinfrastruktur antreiben müssen. Erfahrungen aus Teilprojekten können aber dabei helfen, die Komplexität zu beherrschen – ob das erst mal IRM mit Fokus auf einen Anwendungsfall oder einen Teil der Infrastruktur wie besonders kritische Teile der Microsoft SharePoint-Umgebung ist, ist dabei sekundär.

Fazit

Wichtig ist vor allem, dass sich das Thema IRM überhaupt auf der IT-Agenda befindet, und zwar im Kontext einer Gesamtstrategie für die Informationssicherheit. IRM ist ein wichtiges Element, um Informationen besser schützen zu können. Es erweitert die Sicherheit im Vergleich mit klassischen, etablierten Ansätzen. Allerdings muss der Schritt in Richtung IRM bei der Information und nicht der Technologie ansetzen. Welche Informationen sind schützenswert und wie lassen sich Informationen klassifizieren? Welche Prozesse der Informationsverarbeitung, -nutzung und -weitergabe müssen in besonderer Weise gesichert werden? Und wie lässt sich dieses Thema für die Nutzer vereinfachen und deren Wissen darüber, welche Information wie geschützt werden muss, nutzen, um die zentralen Richtlinien zu verfeinern?

IRM ist keineswegs nur ein technisches Projekt, sondern in hohem Maße ein organisatorisches Thema, da es den Umgang von Organisationen mit Informationen unmittelbar beeinflusst. Dieser Blickwinkel ist aber ein kritischer Erfolgsfaktor für IRM-Lösungen – und diese sind wiederum ein kritischer Erfolgsfaktor für das Thema Informationssicherheit. An IRM führt letztlich kein Weg vorbei. Allerdings haben die Hersteller noch einige Hausaufgaben zu machen, insbesondere im Hinblick auf die Standardisierung, damit IRM zu einer Erfolgsgeschichte wird. *(dr)*

Migration von Windows-Dateiservern auf SharePoint 2010 (2)

Datenwanderung

von Thomas Joos

Im zweiten Teil unserer Workshopserie konfigurieren wir als letzten Schritt der Datenmigration die Metadaten in SharePoint 2010. Anschließend zeigen wir Wege auf, wie die Daten vom alten Fileserver in das neue System wandern. Sehr komfortabel erreichen wir dies unter Windows Server 2008 R2, indem wir die Dateiklassifizierungsdienste einsetzen. Aber auch ohne die neueste Version des Windows Servers gehen die Daten per Skript oder Zusatztool komfortabel auf Wanderung in ihre neue Heimat.

Die zahlreichen Vorarbeiten aus dem ersten Teil unserer Workshopserie müssen wir – vor der eigentlichen Migration der Daten – um einen letzten Schritt ergänzen. Denn auf dem SharePoint-Server fehlt noch die Einrichtung der Metadaten, der wir uns nunmehr zuwenden.

Metadaten nutzen und konfigurieren

Um Dokumente schneller zu finden und einordnen zu können, stellen Metadaten einen effizienten Weg dar. Wie bereits in Windows Vista und 7 lassen sich auch für Dokumente in SharePoint 2010 Metadaten zuordnen, um das Wissen im Unternehmen besser zu katalogisieren. SharePoint 2010 ermöglicht jetzt auch eine zentrale Vorgabe der Metadaten (Taxonomie) und auch die zentrale Verwaltung dieser Metadaten. Alternativ können Anwender auch selbst Stichwörter für Dokumente eingeben (Folksonomie). SharePoint speichert alle Daten zentral und ermöglicht die Nutzung der Kennwörter und Metadaten für alle Benutzer. Metadaten lassen sich dann zum Filtern, zur Suche und als Navigationsbereich nutzen.

In SharePoint haben Anwender selbst die Möglichkeit, den Dokumenten Stichwörter zuzuordnen. Diese lassen sich dann in der SharePoint-Suche nutzen. Da SharePoint die Stichwörter zentral speichert, stehen diese auch anderen Anwendern zur Verfügung. Sobald ein Anwender ein Stichwort eingeben will, das bereits vergeben ist, macht SharePoint einen Vorschlag. Die Stichwörter lassen sich in den Eigenschaften von Dokumenten direkt in der Dokumentenbibliothek vergeben. Anwender können in der Webseite der Dokumentenbibliothek über "Eigenschaften bearbeiten" jedem Dokument eine weitere Eigenschaft als Metadaten hinzufügen. Diese Unternehmensstichwörter speichert SharePoint zentral und ermöglicht die Weiterverwendung durch andere Anwender. Eine weitere Möglichkeit der Metadatenpflege ist die zentrale Speicherung und Vorgabe von Metadaten und trägt die Bezeichnung Taxonomie. Im unteren Bereich der Metadatenpflege eines Dokuments können Administratoren beliebige Spalten integrieren und Ausdrücke vorgeben, die Anwender beim Klassifizieren festlegen müssen. Die Eingaben können freiwillig sein oder können als erzwungen konfiguriert werden. Klicken Anwender auf das kleine Symbol am Ende der Spalte, zeigt SharePoint alle Stichwörter an, die Administratoren für die entsprechende Spalte vorgeben.

SharePoint bietet dafür ein eigenes Verwaltungstool an, das Terminologiespeicher-Verwaltungstool. In diesem Tool legen Sie eigene Stichwörter fest. Diese Stichwörter können Verwalter von Dokumentenbibliotheken einbinden und verwenden. Die Technik trägt in SharePoint 2010 die Bezeichnung "Managed Metadata Services" (verwalteter Metadatendienst). In der Verwaltung der Metadaten durch das Terminologiespeicher-Verwaltungstool sehen Sie auch die Stichwörter, die Anwender in SharePoint selbst vergeben und können diese in die verwaltete Struktur einbinden. Haben Anwender die Metadaten gepflegt, können Sie die Spalten der verwalteten Metadaten schnell und einfach zur Navigation freigeben. Um diese Möglichkeiten zur Verfügung zu stellen, klicken Sie auf der Registerkarte "Bibliothek" in der Dokumentenbibliothek die Schaltfläche "Bibliothekseinstellungen" im Menüband. Hier findet sich der Link "Navigationseinstellungen für Metadaten". Sie können anschließend auswählen, welche Spalten aus den verwalteten Metadaten für die Filterung zur Verfügung stehen sollen, indem Sie diese im Bereich "Navigationshierarchien" einblenden. Über Schlüsselfilter können Sie ein weiteres Webapp anzeigen lassen, in dem die Anwender nach speziellen Begriffen innerhalb der Metadaten suchen können. Klicken Anwender auf einen Ausdruck in der Navigationsleiste, bringt SharePoint nur noch die Dokumente der Bibliothek auf den Schirm, die den entsprechenden Ausdruck als Metadaten hinterlegt haben. Das bedeutet, Sie können in SharePoint komplett auf Ordner verzichten, wenn Sie dafür die Metadatenpflege konfigurieren.

Erstellen Anwender in der Dokumentenbibliothek über die Registerkarte "Doku-

mente" mit "Neues Dokument" eine neue Datei, öffnet sich Word und es lassen sich bereits an dieser Stelle die notwendigen Metadaten hinterlegen. Nach der Erstellung des Dokumentes startet Word und zeigt im oberen Bereich die notwendigen Daten an, die Anwender eintragen können. Wollen Sie Dokumente effizient bereitstellen, sollten Sie sich natürlich nicht auf die Stichworte der Anwender verlassen, sondern können zentral notwendige Stichworte und Sortiermöglichkeiten vorgeben.

Metadaten-Dienst und Inhaltstyp-Hub erstellen

Wollen Sie die zentralen Metadaten verwalten, benötigen Sie das bereits erwähnte Terminologiespeicher-Verwaltungstool (Term Store Management Tool). Dieses starten Sie über die Zentraladministration. Im Bereich "Anwendungsverwaltung" finden Sie den Link "Dienstanwendungen verwalten". Im folgenden Fenster klicken Sie auf "Verwalteter Metadatendienst". Ist ein solcher Dienst noch nicht vorhanden, können Sie einen neuen erstellen, indem Sie auf "Neu / Verwalteter Metadatendienst" klicken. Durch den neuen Inhaltstyphub lassen sich die Inhaltstypen einer Websitesammlung zu anderen Websitesammlungen und Farmen replizieren. Das ist vor allem dann sinnvoll, wenn Sie mehrere Websitesammlungen mit Dokumentenbibliotheken betreiben, aber den verwalteten Metadatendienst für alle Sammlungen nutzen wollen.

Die Konfiguration eines solchen Inhaltstyphubs ist sehr einfach. Sie müssen für einen verwalteten Metadatendienst einfach nur die URL der zentralen Websitesammlung hinterlegen, in der Sie die Inhaltstypen erstellen und zu anderen Websitesammlungen replizieren wollen. Nachdem Sie den Dienst erstellt haben, sehen Sie diesen in den Dienstanwendungen. In der Liste befindet sich der Dienst zweimal: Der obere Eintrag spezifiziert den Dienst selbst, der untere Eintrag steht für die Anbindung von Websitesammlungen an den Dienst, um die Metadaten zu nutzen. Wollen Sie den Dienst konfigurieren, müssen Sie daher den oberen Link verwenden. Markieren Sie die Spalte mit dem Dienst nur und klicken nicht die hinterlegte URL an, können Sie im oberen Bereich über das Menüband die Einstellungen des Dienstes anpassen, die Sie bereits bei der Erstellung festgelegt haben. Klicken Sie direkt auf den Link für den verwalteten Metadatendienst, startet das Terminologiespeicher-Verwaltungstool. Unter "Eigenschaften" des Verbindungsdienstes des verwalteten Metadatendienstes, also dem zweiten Eintrag in der Liste, sehen Sie die Einstellungen für die Verbindungen zu der entsprechenden Websitesammlung. Wichtig ist, dass die Option "Nutzt Inhaltstypen aus dem Inhaltstypkatalog unter {URL der Websitesammlung}" aktiviert ist. Über diesen Weg können Sie für jede Websitesammlung die Replikation von der zentralen Websitesammlung replizieren. Welche Inhaltstypen Sie replizieren wollen, konfigurieren Sie dann in den Websiteeinstellungen der entsprechenden Website. Hier legen Sie für jeden einzelnen Inhaltstyp fest, ob er repliziert werden soll. Beim Erstellen eines verwalteten Metadatendiensts verbindet sich dieser mit der Webanwendung, in der Sie den Dienst erstellen.

Um schließlich den Dienst selbst zu konfigurieren und Schlüsselwörter und Sätze zu erstellen, klicken Sie auf den Namen des neuen Dienstes. Es öffnet sich anschließend das Terminologiespeicher-Verwaltungstool. Zunächst klicken Sie mit der rechten Maustaste auf den Namen des neuen Dienstes und erstellen mit "Neue Gruppe" eine übergeordnete Instanz für ihre verwalteten Schlüsselwörter (Ausdrücke, Terms) und Ausdrucksätze (Term Sets). Haben Sie mehrere Sprachpakete installiert, können Sie für jede Sprache einen eigenen Speicher mit Metadaten verwalten und pflegen. Sobald Sie die Gruppe eingerichtet haben, erscheint diese im unteren Bereich und Sie können über das Kontextmenü neue Ausdrucksätze sowie neue Ausdrücke erstellen. Sie können auf diesem Weg beliebig viele Gruppen anlegen, die dann verschiedene Ausdrucksätze und Ausdrücke enthalten. Die Ausdrucksätze weisen Sie dann später einer neuen Spalte in der Dokumentenbibliothek zu.

Über das Kontextmenü der neuen Gruppe können Sie auch Ausdrucksätze importieren. Dazu fertigen Sie eine CSV-Datei an, welche die notwendigen Ausdrucksätze enthält. Sie können sich den Aufbau einer solchen Datei als Beispiel anzeigen lassen, wenn Sie auf den Namen des Dienstes klicken und dann im Bereich "Beispielimport" mit der rechten Maustaste auf "Beispielimportdatei anzeigen" und dann "Ziel speichern" klicken. Nachdem Sie die Ausdrücke und Ausdrucksätze festgelegt haben, die Sie im Unternehmen nutzen wollen, können Sie diese zur Auswahl in die einzelnen Websites und Dokumentenbibliotheken einbinden.

Dazu müssen Sie festlegen, welche Inhaltstypen diese Metadaten nutzen sollen (also Dokumente, Bilder, selbst erstellte Vorla-

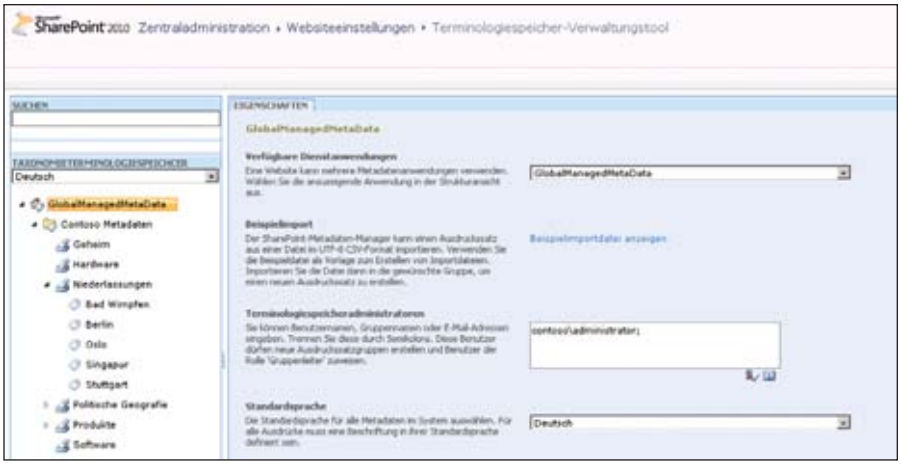


Bild 1: Zentrale Konsole zur Verwaltung der Metadaten

gen et cetera). Erst nach dieser Einbindung stehen diese Daten zur Verfügung. Damit Websites und Dokumentenbibliotheken die konfigurierte Taxonomie auch nutzen, müssen Sie zunächst die Websiteeinstellungen der Seite aufrufen. Diese erreichen Sie über die Schaltfläche "Websiteaktionen" oben links auf der Seite, also nicht in der Zentraladministration. Wenn Sie im Unternehmen viele Inhaltstypen einsetzen und diese auch anderen Websitesammlungen zur Verfügung stellen wollen, sollten Sie eine eigene Websitesammlung erstellen, die Sie ausschließlich für die Pflege der Inhaltsdaten nutzen. Andere Websitesammlungen können die Inhaltstypen der Quell-Websitesammlung dann abrufen und abonnieren. Sie konfigurieren dazu die Quell-Websitesammlung als Inhaltstyphub.

Im neuen Fenster klicken Sie im Bereich "Galerien" auf "Websiteinhaltstypen". Sie müssen die Inhaltstypen festlegen, für welche die Ausdrücke und Schlüsselwörter zur Verfügung stehen, also Dokumente, Bilder und so weiter. Sie erledigen dies entweder über den Link "Einen neuen Inhaltstyp erstellen" oder Sie klicken im Bereich "Dokumenteninhaltstypen" auf "Dokument" beziehungsweise auf den Inhaltstyp, für den Sie die Pflege der Metadaten aktivieren wollen. Sie haben die Möglichkeit, über den Link "Aus neuer Websitespalte hinzufügen" eine weitere Spalte der Bibliothek hinzuzufügen. Diese Spalte zeigt SharePoint dann in den Navigationsbereichen an und stellt diese in den Eigenschaften des Dokuments zur Verfügung, damit Anwender diese bearbeiten können. Hier können Sie dann zum Beispiel einen Ausdrucksatz hinterlegen, den Sie im Verwaltungstool vorgegeben haben. Wichtig ist, dass Sie bei der Konfiguration der Spalte die Option "Verwaltete Metadaten als Informationstyp" auswählen. Anschließend können Sie im Bereich "Ausdrucksatzeinstellungen" auswählen, welche der erstellten Metadaten, also welcher Ausrucksatz, dieser Spalte zugeordnet sein sollen. Anwender können anschließend beim Bearbeiten der Metadaten von Dokumenten den Ausdrucksatz auswählen und die einzelnen Ausdrücke aktivieren, die Sie im Ausrucksatz hinterlegt haben. Auf diese Weise können Sie beliebige Spalten erstellen und den Seiten verschiedene Ausdrucksätze zuordnen.

Damit Inhaltstypen zur Verfügung stehen, auch neue, die Sie erstellen, müssen Sie erst deren Veröffentlichungseinstellungen bearbeiten. Denn erst wenn Sie die Einstellungen veröffentlichen, stehen diese zur Verfügung. Diese finden Sie über den Link "Veröffentlichung für diesen Inhaltstyp verwalten" in den Einstellungen des Inhaltstyps. Achten Sie darauf, dass der gewünschte Inhaltstyp veröffentlicht ist und klicken Sie auf "OK". Rufen Sie die Einstellung erneut auf, können Sie die Veröffentlichung aufheben oder nach Änderungen erneut veröffentlichen. Im Fenster sehen Sie dann auch den Zeitraum der letzten Veröffentlichung und ob diese erfolgreich war. Auch wenn Sie einen bereits vorhandenen Inhaltstyp auf die Unterstützung von Metadaten konfigurieren, müssen Sie diesen erst veröffentlichen. Auf den Websitesammlungen, die Inhaltstypen von der Quell-Website abonniert haben, sehen Sie über "Websiteaktionen / Websiteeinstellungen" im Bereich "Websitesammlungsverwaltung" durch Klicken auf den Link "Inhaltstypveröffentlichung", welche Inhaltstypen die Websitesammlung abonniert hat. Änderungen übernimmt SharePoint allerdings nicht sofort, sondern bindet diese in zeitgesteuerte Aufgaben ein, die nach einiger Zeit gestartet werden. Diese finden Sie in der Zentralverwaltung unter "Überwachung". Um die Zeitaufträge zu steuern, klicken Sie bei "Zeitgeberaufträge" auf "Auftragsdefinitionen überprüfen". Klicken Sie auf eine Aufgabe, öffnet sich deren Einstellungsfenster. Drücken Sie zum Beispiel auf "Jetzt ausführen", startet SharePoint die Änderung sofort. So sollten Sie für die Aufträge Inhaltstyphub und Inhaltstypabonnent vorgehen, wenn Sie Änderungen vorgenommen haben. Anwender können auf diese Weise nicht nur Metadaten pflegen, sondern können die Dokumentenbibliothek so filtern, dass nur noch Dokumente zu sehen sind, die den ausgewählten Ausdruck aufweisen. In den Webparts sehen dann die Anwender genau die gleichen Spalten wie in den Dokumenteneigenschaften und können diese zum Filtern und Suchen verwenden.

Administratoren können für einzelne Metadatenspalten festlegen, dass diese zwingend ausgefüllt werden müssen. Speichert ein Anwender ein Dokument ab, ohne die

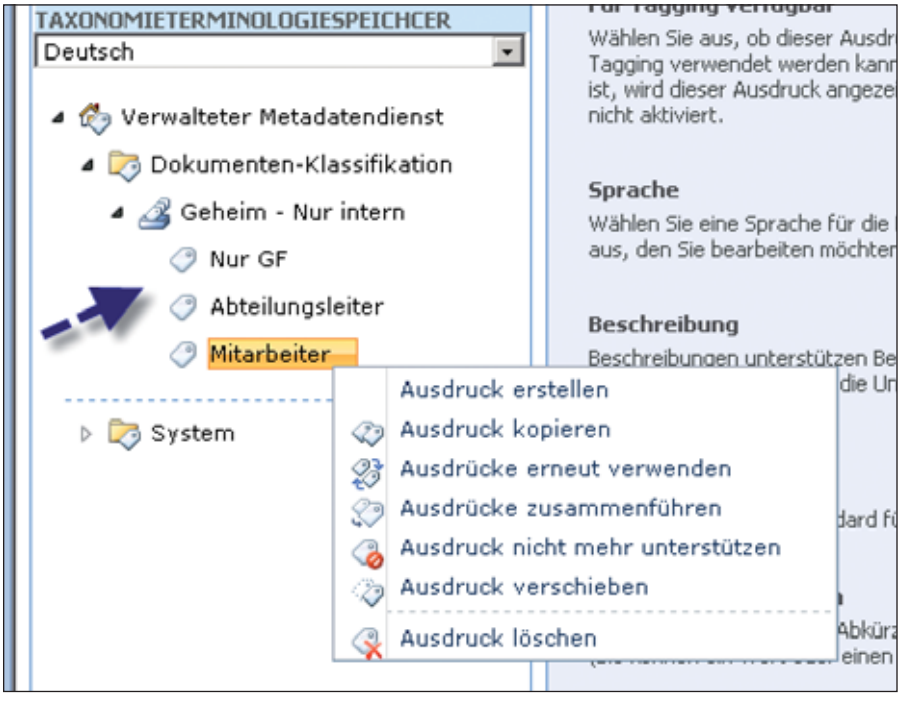


Bild 2: Die zentrale Pflege der Metadaten ermöglicht die Verteilung in einer Webserverfarm

Metadaten zu hinterlegen, erhält er einen Hinweis und Word springt automatisch zum entsprechenden Feld. Sie nehmen diese Einstellungen in der Website vor, in der Sie die Dokumentenbibliothek betreiben. Klicken Sie dazu in der Bibliothek auf die Registerkarte "Bibliothek". Anschließend sehen Sie das Menüband, in dem Sie die Einstellungen der Bibliothek anpassen. Dazu klicken Sie auf die Schaltfläche "Bibliothekeinstellungen". Im Bereich Spalten sehen Sie die einzelnen Metadaten, die zur Verfügung stehen. Wollen Sie sicherstellen, dass Benutzer einzelne Metadaten zwingend ausfüllen, klicken Sie auf die Spalte. Sie können an dieser Stelle verschiedene Einstellungen ändern. Aktivieren Sie zum Beispiel "Diese Spalte muss Informationen enthalten", müssen Anwender die Daten auch auswählen, die Sie über die Taxonomie vorgeben.

Dateiklassifizierungsdienste

Vor allem Unternehmen, die planen, Dokumente vom Dateisystem der Server über SharePoint zur Verfügung zu stellen, stehen vor dem Problem, die Metadaten der Dokumente zu steuern. Da SharePoint 2010 sehr gut mit Metadaten umgehen kann, ist es sehr sinnvoll, diese Daten zu pflegen. Allerdings müssen Metadaten manuell mit Dokumenten verbunden werden. Setzen Sie jedoch Windows Server 2008 R2 ein, können Sie die Metadaten automatisiert über Regeln festlegen lassen. Die neuen Dateiklassifizierungsdienste (File Classification Infrastructure, FCI) in Windows Server 2008 R2 können bestehende Dokumente untersuchen, Inhalte feststellen und entsprechende Richtlinien anwenden sowie Metadaten festlegen. Dazu können Sie Dokumenten zusätzliche Eigenschaften zuweisen wie in SharePoint. Die Eigenschaften liegen direkt im Dokument, nicht im NTFS-Dateisystem. Laden Sie solche Dokumente in SharePoint hoch, sind die Metadaten weiter verfügbar. Die Dateiklassifizierungsdienste gehören zum Rollendienst Ressourcen-Manager für Dateiserver. Sie verwalten daher diese Funktion auch über die Verwaltungskonsole des Ressourcen-Managers für Dateiserver (FSRM).

Im Zusammenspiel der genannten Komponenten haben Sie vor allem den Vorteil, Metadaten bereits automatisch im Dateisystem der Dateiserver zu pflegen, nicht erst in SharePoint. Damit Sie den Ressourcen-Manager für Dateiserver nutzen können, müssen Sie ihn im Server-Manager als Rollendienst der Serverrolle Dateidienste installieren. Sie starten den Ressourcen-Manager für Dateiserver über die Programmgruppe "Verwaltung" oder über *fsrm.msc*. Über den Menüpunkt "Klassifizierungsverwaltung" verwalten Sie die Dateiklassifizierung und legen Regeln für Metadaten fest. Die Basis der Metadaten sind die Klassifizierungseigenschaften. Hier legen Sie die Metadaten fest, die Sie für die Dokumente auf den Dateiservern pflegen wollen. Die Eigenschaften verhalten sich ähnlich zu den Eigenschaften von Dateien in SharePoint. Klicken Sie mit der rechten Maustaste auf "Klassifizierungseigenschaften", können Sie mit "Eigenschaft erstellen" festlegen, welche neuen Kriterien Dateien zugeordnet werden sollen, also erste Metadaten. So lässt sich zum Beispiel festlegen, ob ein Dokument zu einem Projekt gehört, private Daten enthält, nur für den internen Gebrauch oder für bestimmte Personen nutzbar sein soll.

Das Anlegen und Bearbeiten von Klassifizierungseigenschaften ändert aber noch keine Dokumente ab, sondern bietet nur die Verwendung der jeweiligen Eigenschaften an. Damit diese auch mit Dokumenten verknüpft werden, müssen Sie Klassifizierungsregeln über deren Kontextmenü erstellen. Mit diesen Regeln bearbeitet Windows Server 2008 R2 die Dokumente und fügt die entsprechenden Markierungen hinzu. Erstellen Sie eine neue Regel, legen Sie zunächst fest, welchen Namen die Regel hat und welche Verzeichnisse im Dateisystem die Regel berücksichtigen soll. Auf der Registerkarte "Klassifizierung" definieren Sie, dass Sie Dateien mit der Ordnerklassifizierung ändern wollen und wählen die erstellte Klassifizierungseigenschaft und den Wert aus, den der Server den Dateien zuordnen soll. Anschließend stempelt die Regel alle Dateien in den entsprechenden Ordnern automatisch mit den hinterlegten Eigenschaften.

Über den Menüpunkt "Klassifizierungszeitplan konfigurieren" im Kontextmenü der Klassifizierungsregeln können Sie festlegen, wann Klassifizierungsregeln starten sollen, ob Sie einen Bericht erhalten wollen und wenn ja, in welchem Format, sowie zahlreiche weitere Einstellungen. Klassifizierungsregeln werden durch Klassifizierungszeitpläne gesteuert. Speichern Anwender neue Dokumente in den entsprechenden Verzeichnissen, stempelt der Server automatisch die Dateien mit den entsprechenden Metadaten. Die Klassifizierungsregeln verwenden dann wiederum die Klassifizierungseigenschaften. Sie können die Regeln an dieser Stelle auch sofort ausführen lassen. Es steht Ihnen frei, mehrere Regeln zu erstellen und auch komplexere Regeln anzuwenden. Auch das

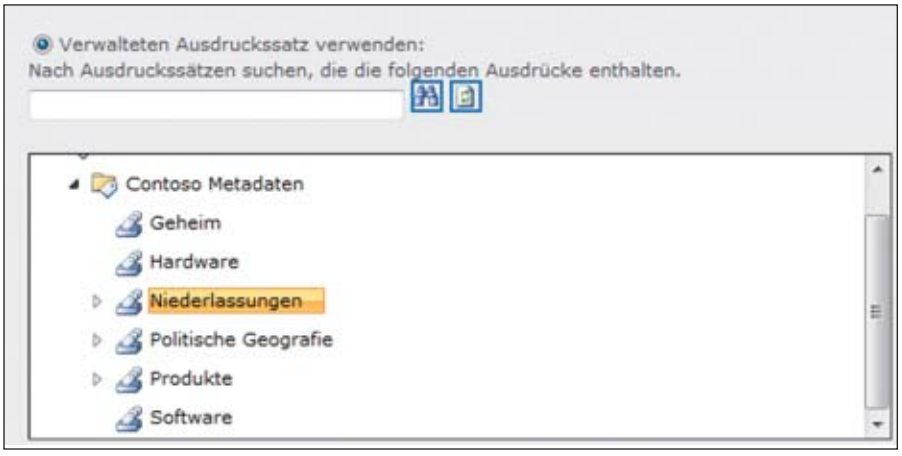


Bild 3: Zuordnen von Ausdruckssätzen zu den Spalten eines Inhaltstyps

Bleiben Sie in Verbindung!

Folgen Sie uns auf Twitter

twitter.com/ita_blog

Werden Sie ein Fan auf Facebook

www.facebook.de/itanet

Treten Sie unserer Xing-Gruppe bei

www.xing.com/net/itanet

Lesen Sie unseren RSS-Feed

www.it-administrator.de/rss.xml

Social Networks sind auch beim IT-Administrator angekommen!

Auf Facebook haben wir ein eigenes Profil. Neben ausgesuchten Informationen rund um das Magazin und Veranstaltungshinweisen finden Sie hier auch Gewinnspiele oder Wissenstests. Oder wollen Sie den IT-Administrator in 140 Zeichen täglich begleiten? Verfolgen Sie unser „Gezwitscher" über die interessantesten Neuigkeiten, besten Downloads und Tipps auf Twitter. Wenn Sie aber den direkten Austausch suchen, sind Sie in unserer Xing-Gruppe genau richtig. Lernen Sie dort Ihre Kollegen aus der IT und die Heftmacher des IT-Administrators persönlich kennen und nehmen Sie Einfluss auf Ihr Praxismagazin. Immer gut informiert bleiben Sie auch über unseren RSS-Feed.

Treten Sie unserer Community bei. Wir freuen uns auf Sie.

iT administrator

Das Magazin für professionelle System- und Netzwerkadministration

Zuteilen von einzelnen Eigenschaften zu Dateien ist möglich. Haben Sie Dokumente auf dem Dateisystem mit Metadaten versorgt, können Sie über die Inhaltsorganisation Regeln festlegen, welche die Dokumente auf Basis der hinterlegten Metadaten in speziellen Ordnern speichert. Dazu müssen Sie einfach zusätzliche Regeln für den Inhalt erstellen und diese auf die Metadaten der Klassifizierungsverwaltung anbinden.

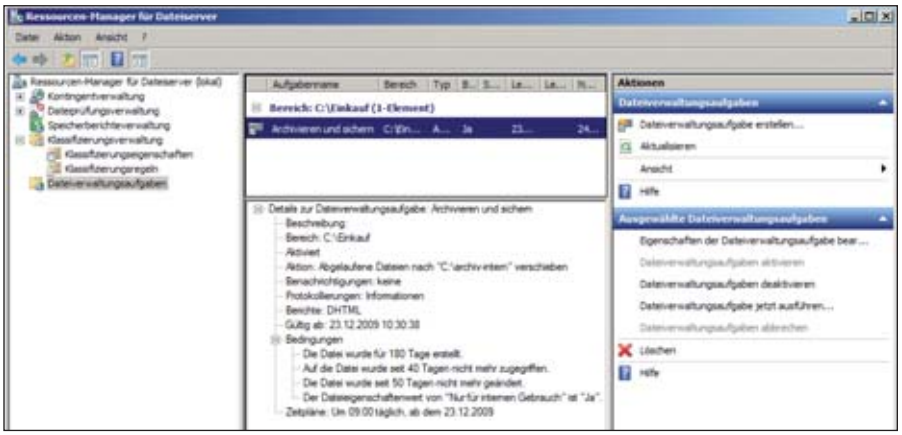


Bild 4: Die Dateiklassifizierung in Windows Server 2008 R2 vereinfacht die Migration nach SharePoint 2010 erheblich

Automatische Dateiorganisation mit Inhaltsorganisation

Eine weitere neue Funktion in SharePoint 2010 ist die Inhaltsorganisation. Diese Funktion kann Dokumente automatisch auf Basis bestimmter Regeln und auf Basis von Metadaten, Inhaltstypen oder Namen an den Orten speichern, die Sie vorher festlegen. Sie können dazu verschiedene Bibliotheken, Ordner und Websites zur Speicherung verwenden. Der Organizer routet sozusagen Dokumente anhand der hinterlegten Metadaten oder des Inhaltstyps in die richtige Bibliothek oder Ordner. Sobald Anwender ein Dokument hochladen, prüft SharePoint die Metadaten, Inhaltstyp und andere Eigenschaften, die Sie vorgeben, und speichert das Dokument entsprechend definierter Regeln ab.

Um die Inhaltsorganisation verwenden zu können, müssen Sie zunächst die Features der Websitesammlung, in der Sie die Inhaltsorganisation nutzen wollen, bearbeiten. Klicken Sie dazu auf "Websiteaktionen / Websiteeinstellungen" und dann im Bereich "Websitesammlungsverwaltung" auf "Websitesammlungsfeatures". Auf dieser Seite müssen Sie sicherstellen, dass einer der beiden Dienste "Features von SharePoint Server-Standardwebsite-Sammlungen" oder "Features von Websitesammlungen in SharePoint Server Enterprise" aktiviert ist. Erst dann können Sie die Inhaltsorganisation einsetzen.

Nachdem Sie dies sichergestellt haben, rufen Sie über "Websiteaktionen / Websiteeinstellungen" im Bereich "Websiteaktionen" den Link "Websitefeatures verwalten" auf. Hier können Sie jetzt das Feature "Inhaltsorganisation" aktivieren. Anschließend starten Sie die Verwaltung dieses Features über die beiden Links "Einstellungen der Inhaltsorganisation" und "Regeln für die Inhaltsorganisation" im Bereich Websiteverwaltung. Haben Sie das Feature aktiviert, legt SharePoint außerdem eine neue Bibliothek mit der Bezeichnung "Abgabebibliothek" an. Klicken Sie zur Verwaltung der Inhaltsorganisation zunächst auf den Link "Einstellungen der Inhaltsorganisation" in der Websiteverwaltung über "Websiteaktionen / Websiteeinstellungen". Hier treffen Sie Einstellungen, die generell für die Inhaltsorganisation dieser Website gelten. Über den Link "Regeln für die Inhaltsorganisation" in der Websiteverwaltung über "Websiteaktionen / Websiteeinstellungen" legen Sie Regeln für eintreffende Dokumente fest, wie etwa die Bedingungen und die Ziel-Bibliothek.

Aktivieren Sie die Option "Automatisch einen Ordner…erstellen", um ähnliche Dokumente in Ordnern zusammenzufassen. Die Spalte im entsprechenden Inhaltstyp, auf die Sie die Bedingung aufbauen, muss als erforderlich definiert sein. Ist die Spalte nur optional, lassen sich Ordner nicht automatisch erstellen. Laden Anwender ein Dokument in der Abgabebibliothek hoch, erhalten die Anwender die Information, dass SharePoint auf Basis von Regeln das Dokument entsprechend in der korrekten Bibliothek und Ordner ablegt. Sobald das Dokument ausgewählt ist, erscheint das Fenster, in dem die Anwender die Metadaten pflegen. Sobald die Speicherung abgeschlossen ist, erhalten Anwender eine Information, dass das Dokument abgelegt ist mit einem Link, wo das Dokument zu finden ist.

Daten aus Dateiservern zu SharePoint übernehmen

Neben der Vorbereitung der Serverfarm und Bibliotheken ist es in vielen Fällen notwendig, dass Administratoren große Mengen an Dokumenten von den Netzwerkfreigaben in die SharePoint-Bibliotheken übernehmen müssen. Bei dieser Aufgabe besteht die Möglichkeit, die Daten einzeln zu übernehmen oder zu automatisieren. SharePoint 2010 erlaubt für Bibliotheken auch, mehrere Dateien auf einmal hochzuladen. Ist der manuelle Upload nicht möglich, helfen bei der Migration Zusatztools. Die bekanntesten Werkzeuge finden Sie in der Tabelle "Tools für die Dateiservermigration". Nicht alle Tools dienen der direkten Übernahme von Daten aus Dateiservern, sondern haben eher den Fokus, Daten von Vorgängerversionen von SharePoint 2010 zu übernehmen. In diesem Fall stellt der entsprechende Hersteller aber meistens auch ein Tool für die Migration von normalen Dateispeicherorten zu SharePoint bereit.

FCI SharePoint Upload-Skript

Microsoft bietet ein kostenloses Skript [1] zum Upload von Dokumenten an. Das Skript hat allerdings den Nachteil, ziemlich komplex zu sein, da sich Administra-

toren zum einen mit den neuen Dateiklassifizierungsdiensten auseinandersetzen müssen und zum anderen mit der PowerShell sowie den Rechten im Dateisystem und in SharePoint. Das Skript funktioniert ausschließlich mit Windows Server 2008 R2. Für den Upload verwendet das PowerShell-Skript Metadaten, die Sie über die Dateiklassifizierungsdienste für Freigaben definiert haben, beziehungsweise Dateiverwaltungsaufgaben, ein Teil der Dateiklassifizierungsdienste.

Das Produkt ist eigentlich für SharePoint Server 2007 gedacht, funktioniert aber mit Einschränkungen auch in SharePoint Server 2010. Diese Einschränkungen bestehen allerdings nur darin, dass Metadaten verloren gehen können oder etwas durcheinander kommen. Außerdem setzt SharePoint teilweise den Zeitstempel der Datei zurück. Um Daten von einem Server über das Skript in SharePoint-Bibliotheken zu übernehmen, müssen Sie den Ressourcen-Manager für Dateiserver als Rollendienst der Rolle Dateiserver installiert haben. Außerdem muss die Bibliothek, in die Sie Daten übernehmen wollen, vorher angelegt sein und der Benutzer, mit dem Sie Dokumente hochladen, muss Rechte für den Upload in der Bibliothek erhalten. Zusätzlich bietet es sich an, dass Sie für das Skript nicht direkt die PowerShell verwenden, sondern die Skriptumgebung PowerShell ISE. Diese müssen Sie als Feature über den Server-Manager installieren.

Der Vorteil des Skripts ist, dass Sie Dateien auch mit Hilfe der Inhaltsorganisation hochladen können. Um das Skript zu testen, kopieren Sie am besten dessen Inhalt in eine neue Textdatei, die Sie mit dem Editor erstellt haben. Markieren Sie alles ab den Kommentaren, die mit "#" gekennzeichnet sind. Benennen Sie die Datei anschließend in *FciSharePointUpload.ps1* um und kopieren Sie diese auf dem Server, auf dem Sie den Upload testen wollen. Bevor Sie den Upload eines ganzen Verzeichnisses durchführen, sollten Sie in der PowerShell oder der PowerShell ISE zunächst eine Datei hochladen, um Fehler zu vermeiden. Die Syntax eines solchen Befehls ist zum Beispiel:

```
c:\windows\FciSharePointUpload.ps1
  -file "c:\vertrieb\auftrag.vsd"
  -url "http://sps01" -libPath
  "Vertrieb" -sourceAction url -user
  contoso\administrator -password
  hallohallo
```

Haben Sie die Befehle korrekt eingegeben und kann der Befehl auf die lokale Datei sowie die Bibliothek zugreifen, sollte sich die Datei nach wenigen Sekunden in der Bibliothek befinden. Im Quell-Verzeichnis legt das Skript automatisch eine Verknüpfung zur Datei in der Bibliothek an. Das heißt, sobald ein Anwender diese Datei anklickt, öffnet sich diese in der Bibliothek. Dieses Verhalten können Sie mit der Option "-sourceAction" steuern.

Hochladen von Dokumenten mit der PowerShell

Wollen Sie den Benutzernamen und das Kennwort nicht in den Befehl mit aufnehmen, können Sie hier mit einer Variablen arbeiten. Geben Sie *$auth = get-credential* ein, erscheint ein Authentifizierungsfenster. Hier geben Sie die Daten des Benutzers ein, mit dem sich das Skript mit der Bibliothek und dem Verzeichnis verbinden soll. Geben Sie dann den Befehl

```
c:\windows\FciSharePointUpload.ps1
  -file "c:\vertrieb\kunden.docx"
  -url "http://sps01" -libPath "Ver-
  trieb" -sourceAction url -user
  $auth
```

ein, um die Daten aus der Variablen zu verwenden. Auf diese Weise können Sie übrigens mit allen CMDlets der PowerShell arbeiten, die eine Authentifizierung benötigen. Sie müssen bei der Ausführung des PowerShell-Skriptes darauf achten, wie die Sicherheitsrichtlinie der PowerShell auf dem Server eingestellt ist. Standardmäßig blockiert die PowerShell nicht signierte Skripte über die Ausführungsrichtlinie. Sie können die Ausführungsrichtlinie mit dem CMDlet "Set-ExecutionPolicy" ändern und mit *get-executionpolicy* anzeigen. Die Ausführungsrichtlinie speichert ihre Daten in der Windows-Registrierung, das heißt, Sie müssen diese nur einmal anpassen. Sie können folgende Einstellungen vornehmen:

- Restricted: Standardeinstellung, die keine Skripte erlaubt; SharePoint-Skripte funktionieren nicht.
- AllSigned: Nur signierte Skripte erlaubt. Auch hier funktionieren keine SharePoint-Skripte, da diese nicht signiert sind.
- RemoteSigned: Bei dieser Einstellung müssen Sie Skripte für eine Zertifikatsstelle signieren.
- Unrestricted: Mit dieser Einstellung funktionieren auch die SharePoint-Skripte.

Nach der Eingabe von *Set-ExecutionPolicy unrestricted* müssen Sie die Ausführung noch bestätigen. Neben dem manuellen Upload einer Datei können Sie jetzt diese Aufgabe mit dem Skript automatisieren. Dazu benötigen Sie die Dateiklassifizierungsdienste des Ressourcen-Managers für Dateiserver. Klicken Sie mit der rechten Maustaste auf "Dateiverwaltungsaufgaben" und wählen Sie "Dateiverwaltungsaufgabe erstellen" aus. Geben Sie der Aufgabe einen Namen und eine Beschreibung. Im unteren Teil des Fensters wählen Sie bei Bereich das Verzeichnis aus, dessen Dateien Sie in SharePoint hochladen wollen. Auf der Registerkarte "Aktion" aktivieren Sie den Typ "Benutzerdefiniert". Im Bereich "Ausführbare Datei" verwenden Sie

```
C:\Windows\System32\WindowsPower-
  Shell\v1.0\powershell.exe
```

In der Zeile "Argumente" tragen Sie die entsprechende Zeile ein, die das Skript startet, mit dem die Dateiverwaltungsaufgabe die Dateien des ausgewählten Verzeichnisses in die entsprechende Bibliothek hochlädt, zum Beispiel:

[1] PowerShell-Skript zum Upload von Dokumenten
B1P01

Link-Codes

```
-noninteractive -file
  c:\windows\FciSharePointUpload.ps1
  -file "[Source File Path]" -url
  "http://sps01" -libPath "Vertrieb"
  -sourceAction url -user
  contoso\administrator -password
  hallohallo
```

Die Option "[Source File Path]" sorgt dafür, dass die Dateiverwaltungsaufgabe die Datei hochlädt, die aktuell bearbeitet wird. Diese Variable versteht aber nur der Ressourcenmanager für Dateiserver, Sie können die Option nicht in einer normalen PowerShell verwenden. Achten Sie auf die Anführungszeichen.

Im Bereich "Befehlssicherheit" wählen Sie "Lokales System" aus. Auf der Registerkarte "Bedingung" können Sie noch weitere Bedingungen hinterlegen, wie Windows die Datei ausfiltern soll, zum Beispiel auf Basis von Metadaten, die Sie wiederum vorher mit den Dateiklassifizierungsdiensten festgelegt haben. Über die Registerkarte "Zeitplan" legen Sie fest, wann der Befehl starten soll. Nachdem Sie die Aufgabe erstellt haben, starten Sie diese über das Kontextmenü. Auf der Downloadseite für das Skript erhalten Sie weiterführende Informationen zu allen Optionen. Überprüfen Sie, ob die Aufgabe alle Dateien findet und diese hochlädt. Leider funktioniert das Skript nicht immer zuverlässig, was sich darin äußert, dass die Dateiverwaltungsaufgabe keine Dateien hochlädt. Hier erhalten Sie Hilfe auf der Downloadseite und den hinterlegten Links zum Scripting-Forum.

Zusatztools für die Migration

Da die Übernahme von Dokumenten ein komplizierter Vorgang sein kann, sollten Administratoren entweder manuell Daten übernehmen, Skripte verwenden wie vorher besprochen oder besser auf Tools setzen, die bei der Migration helfen. SharePoint-Projekte sind sicher keine ganz günstigen Projekte. Aus diesem Grund sollten Unternehmen vor allem bei der Datenübernahme wichtiger Dokumente nicht an der falschen Stelle sparen. Für die meisten Tools stellen die Unternehmen umfassende Hilfen sowie Webcasts und Demovideos zur Verfügung. Es ist empfehlenswert, vor der eigentlichen Migration ausführliche Tests der verschiedenen Produkte durchzuführen. Anschließend können Unternehmen auf Basis des Preises und der Leistung des entsprechenden Produktes entscheiden, mit welchem Werkzeug Sie die Datenübernahme durchführen wollen. Welches Tool das richtige ist, hängt vom entsprechenden Unternehmen ab. *(jp)*

Tools für die Dateiservermigration

Toolname	Link-Code	Funktion
Metalogix SharePoint Site Migration Manager 2010	B1P02	Ermöglicht die Migration von SharePoint Server 2003/2007 zu 2010. Das Tool ist leicht zu bedienen und erlaubt das Verschieben von Inhalten zwischen verschiedenen Versionen. Auch Berechtigungen und Webparts lassen sich migrieren. Gestattet standardmäßig keine Datenübernahme von Dateifreigaben. Für diese Aufgabe bietet Metalogix das Tool FileShare Migration Manager 2010 an.
FileShare Migration Manager 2010	B1P03	Migration von Dokumenten aus Dateifreigaben zu SharePoint. Die Migration lässt sich über die PowerShell scripten. Das Tool steht als Demoversion zur Verfügung.
Document Import Kit for SharePoint 2010 / 2007 (DocKIT)	B1P04	Hat die Aufgabe, Daten von Dateifreigaben zu SharePoint zu übernehmen. Das Tool steht als 30 Tage-Demo zur Verfügung.
Quest Migration Manager for SharePoint	B1P05	Ermöglicht die direkte Migration des Inhalts von SharePoint Portal Server 2003 zu SharePoint 2010, inklusive Neuordnung der Struktur. Auch die Migration erleichtert sich dadurch. Für die Migration von Daten aus Dateiservern bietet Quest das Tool Migrate File Shares to SharePoint.
Migrate File Shares to SharePoint	B1P06	Ermöglicht die Datenübernahme von Tools von Dateiservern und Novell-Servern zu SharePoint. Während der Migration lassen sich Metadaten eingeben.
Tzunami Deployer for SharePoint 2010 migration	B1P07	Unterstützt ebenfalls bei der Migration zu SharePoint Server 2010, auch von 2003.
Tzunami Deployer for File Shares Migration	B1P08	Übernahme von Dokumenten aus Dateifreigaben inklusive Metadaten und Berechtigungen.
AvePoint DocAve SharePoint Migration Manager for 2001/2003/2007 to 2003/2007/2010	B1P09	Unterstützt das automatische Verschieben von Inhalten zwischen allen SharePoint-Versionen. Metadaten und Berechtigungen bleiben erhalten, genauso wie Ordnerstrukturen.
DocAve File System Migrator for Microsoft SharePoint	B1P00	Ermöglicht die Datenübernahme von Dateiservern zu SharePoint-Bibliotheken. Die Übernahme lässt sich automatisieren.
MetaVis Migrator for SharePoint	B1P0A	Kann ebenfalls Daten zwischen allen SharePoint-Versionen verschieben, inklusive Anpassung der Strukturen. Auch die Anbindung von Freigaben im Netzwerk ist möglich. Im Gegensatz zu vielen anderen Herstellern sind bei MetaVis alle diese Möglichkeiten bereits integriert. Sie benötigen nicht mehrere Produkte für die Migration.
Xavor SharePoint 2010 Migration Tool	B1P0B	Das kostenlose Tool unterstützt bei der Migration von SharePoint 2007 zu 2010 für Datenbanken bis zu 30 GByte. Das Tool ermöglicht allerdings keine Migration von Dateifreigaben.

Kostenlos für IT-Administrator Abonnenten

ITANet

ITANet Workshop-Partner: GIb Gesellschaft für Informationstechnik und -Beratung mbH

ITANet Workshop-Partner: baramundi software AG

Workshop in Augsburg und St. Augustin

Netzoptimierung für Virtualisierung und Storage
am 10. März und 7. April 2011

Die Agenda:

10.00 Uhr: Begrüßung

10.15 Uhr: Switching und Virtualisierung Teil 1

> Switching mit TRILL:
höhere Bandbreite bei niedrigeren Latenzzeiten

> Virtual Ethernet Port Aggregation (VEPA):
vereinfachtes Switching für Server-Netze

> Inter-VM Hairpinning:
effektives Switching für virtualisierte Server

Dozent: Mathias Hein

12.00 Uhr: Partnervortrag: Client-Lifecycle-Management:
Automatisiert zu Windows 7 wechseln

> Vorbereitungen, Aufgaben und Herausforderungen vor dem Betriebssystemwechsel

> Risiken vermeiden mit dem Windows 7-Kompatibilitätscheck

> Windows 7 automatisiert installieren

> Beispielhaftes Migrationsszenario

Dozent: Gerd Conrad, baramundi AG

12.45 Uhr: Mittagspause

14.00 Uhr: Switching und Virtualisierung Teil 2

Dozent: Mathias Hein

15.00 Uhr: Partnervortrag: Weltweite Client-Lifecycle-Unterstützung

> Client-Lifecycle-Management weltweit

> Vorbereitung zum Rollout mit Windows 7

> PXE baramundi Server auf XEN Client unter SLES

Dozent: Michael Terkatz, GIb-mbH

15.45 Uhr: Pause

16.00 Uhr: Mehr Geschwindigkeit im Storage-Netz:

> Fibre Channel vs. iSCSI vs. Fibre Channel over IP:
Einsatzziele und Problemfelder

> Was wird sich langfristig durchsetzen und warum?

Dozent: Mathias Hein

17.30 Uhr: Ende der Veranstaltung

Termin: 10. März 2011
Ort: Baramundi Software AG,
Beim Glaspalast 1, 86153 Augsburg
Uhrzeit: 10.00 bis ca. 17.30 Uhr

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos.

Anmeldeschluss: 3. März 2011

Termin: 7. April 2011
Ort: Konrad-Adenauer-Stiftung e.V.,
Rathausallee 12, 53757 Sankt Augustin
Uhrzeit: 10.00 bis ca. 17.30 Uhr

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos.

Anmeldeschluss: 31. März 2011

Mehr Infos und Anmeldeformulare unter
www.it-administrator.de/workshops/


Quelle: Pixelio.de

Sicherheitslücken auf der Spur mit OpenVAS

Ein Ohr am Netzwerk

von Dr. Holger Reibold

Je komplexer die IT-Infrastrukturen, desto schwieriger wird es, mögliche Schwachstellen zu identifizieren und zu schließen. Möchten Administratoren das Netzwerk und die kritischen Systeme auf ihre Zuverlässigkeit hin überprüfen, müssen sie diese wohl oder übel echten Attacken aussetzen. Um sich eine langwierige Ausbildung zum Hacker zu ersparen, sollten Sie zu einem Spezialisten greifen, der all das beherrscht – einem Security-Scanner. Solche Systeme simulieren auf den zu testenden Systemen typische Attacken. Der einzige freie Sicherheitsscanner, der auch professionellen Anforderungen genügt, ist OpenVAS. Als Nachfolger von Nessus ist er ein typischer Vertreter der Netzwerk- oder Vulnerability-Scanner. In diesem Workshop führen wir Sie durch einen Schnelleinstieg in die Software und zeigen auf, wie Sie komfortabel mit vorgefertigten Skripten auch Windows-Systeme auf ihre Sicherheit scannen.

Die Funktionsweise von OpenVAS [1] ist simpel: Beim Start des Servers werden automatisch sogenannte Plug-Ins geladen, mit denen sich diverse Sicherheitslücken des Betriebssystems beziehungsweise der Dienste aufdecken lassen, die auf den zu scannenden Hosts laufen. Der Client stellt eine Verbindung zum Server her und erzeugt eine Session, in der die Plug-Ins, der oder die Ziel-Hosts und weitere Scan-Einstellungen definiert werden. Wurde der Scan auf einem Host ausgeführt, gibt der OpenVAS-Client eine Übersicht über die offenen Ports und eventuell gefundene Sicherheitslücken aus. Das Tool basiert auf einer Client-Server-Architektur. Der Server wird auf einem Linux-System (openvas-scanner) ausgeführt und lässt sich von einem lokalen oder auch entfernten Client steuern.

Die OpenVAS-Architektur

OpenVAS ist ein komplexes Gebilde, bei dem verschiedene Komponenten ineinandergreifen. Der OpenVAS-Server ist das Kernmodul der OpenVAS-Umgebung. Mit diesem Modul können Sie eine große Anzahl von Rechnern testen, und zwar in kurzer Zeit. Die Scans gehen immer von dem Rechner aus, auf dem der OpenVAS-Server ausgeführt wird. Es versteht sich von selbst, dass der Rechner, auf dem der OpenVAS-Server läuft, die zu scannenden Zielrechner erreichen kann. Der Server ist – im Unterschied zu Nessus – nur für Linux-Betriebssysteme verfügbar.

Die zweite wichtige Komponente trägt die Bezeichnung OpenVAS-Libraries. In diesem Modul sind die von OpenVAS genutzten Bibliotheken enthalten. Seit der Einführung von OpenVAS 3.0 ist OpenVAS-LibNASL in den Libraries aufgegangen. Diese Komponente enthält die eigentlichen Sicherheitstests (Network Vulnerability Tests, kurz NVTs). Die Tests, genauer die zugehörigen Skripte, sind in der Nessus Attack Scripting Language, kurz NASL, geschrieben. OpenVAS hat sie also quasi von seinem Vorläufer geerbt. Inzwischen gibt es auch eigene Erweiterungen und Neuerungen.

Dann gibt es noch die Komponente OpenVAS-Plug-Ins, die Ihnen eine Grundausstattung an Testskripten zur Verfügung stellt. Sie sollten allerdings beachten, dass der Updatezyklus dieses Moduls nicht dazu gedacht ist, die Verfügbarkeit aktueller NVTs sicherzustellen. Wenn Sie aktuelle NVTs benötigen, sollten Sie einen NVT-Feed abonnieren.

Als Administrator arbeiten Sie meist mit der vierten Komponente: dem OpenVAS-Client. Er steuert den OpenVAS-Server, verarbeitet die Scanergebnisse und präsentiert Ihnen diese. Wichtig dabei: Der OpenVAS-Client kann auf (nahezu) jedem beliebigen Rechner ausgeführt werden. Der Client ist für Linux und Windows verfügbar. Er baut eine Verbindung zum OpenVAS-Server auf und steuert ihn. Sie können Client und Server natürlich auch auf dem gleichen System ausführen.

Neben diesen Kernmodulen gibt es vier weitere optionale Komponenten:

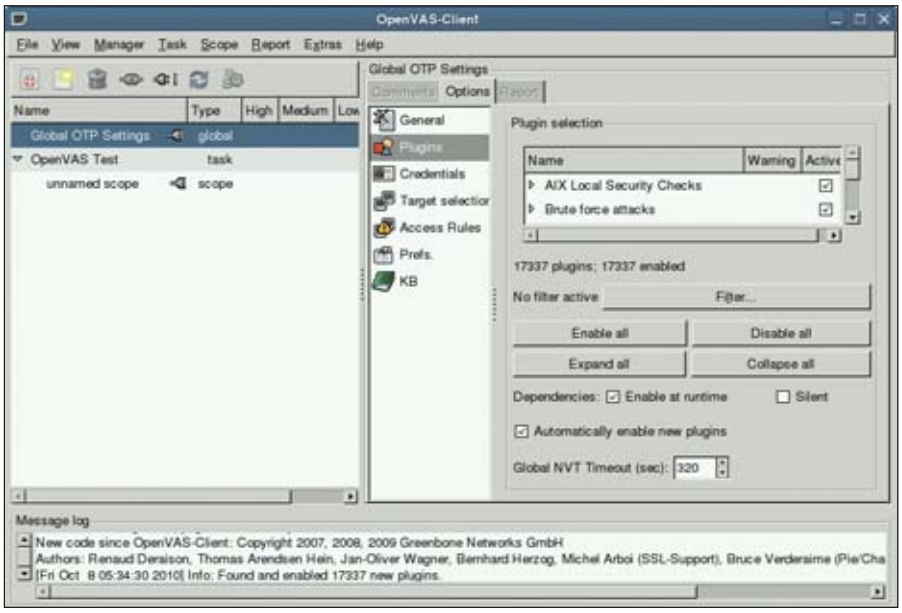


Bild 1: Über den OpenVAS-Client 3.0.1 wird der OpenVAS-Server gesteuert

- OpenVAS-Manager: Dient dem Management der OpenVAS-Installation und verwendet für die Kommunikation das OMP (OpenVAS Management Protocol).
- OpenVAS-Administrator: Diese optionale Komponente dient der Administration der OpenVAS-Umgebung. Sie greift auf das OAP (OpenVAS Administration Protocol) zurück.
- OpenVAS CLI: Die Konsolenvariante (CLI, Command Line Interface) für Anwender, die lieber auf Konsolenebene arbeiten.
- GSA: Mit dem Greenbone Security Assistant steht Ihnen eine tolle webbasierte Umgebung für den Zugriff auf die OpenVAS-Umgebung zur Verfügung.

Der Schnelleinstieg

Das Herzstück von OpenVAS sind die Plug-Ins, also die eigentlichen Testskripte, die an den Zielsystemen die gewünschten Test durchführen (das OpenVAS-Team präferiert den Begriff der NVTs). Diese Skripte sind in über 40 Kategorien unterteilt und inzwischen gibt es mehr als 17.500 Tests. Über den OpenVAS-Client erfolgt die Auswahl der NVT. Mit einem Klick auf die jeweilige Kategorienbezeichnung erkennen Sie, wie viele Plug-Ins einer Kategorie zugeordnet sind. Mit einem Doppelklick auf einen Listeneintrag öffnen Sie die Detailinformationen zu den einzelnen Test-Skripten. Insbesondere über das Register "Options" können Sie eine Vielzahl von Einstellungen anpassen. Unter "Target Selection" bestimmen Sie die Zielsysteme, die Sie unter die Lupe nehmen wollen. Den eigentlichen Scanvorgang leiten Sie mit einem Klick auf die Schaltfläche "Execute" ein. Den Scan-Vorgang zeigt der Client durch rotierende Punkte an. Die Ergebnisse präsentiert Ihnen der Client auf dem Register "Report".

Für das Erstellen von neuen Scan-Konfigurationen können Sie zwei Wege einschlagen: Entweder Sie legen diese in der Scan-Liste an oder aber greifen zu dem Scan-Assistenten, der über die Symbolleiste beziehungsweise das Menü "File / Scan Assistant" verfügbar ist. Nachdem Sie eine erste Testkonfiguration ausgeführt haben, finden Sie Berichte des OpenVAS-Clients auf dem Report-Register. Der Bericht zeigt im linken Bereich die gescannten Systeme an, rechts finden Sie die zugehörigen Detailinformationen. Kritische Ereignisse werden farbig gekennzeichnet und beispielsweise rot markiert. Die Berichtinfo liefert Ihnen in der Regel die notwendigen Informationen, um die (potenzielle) Schwachstelle schließen zu können.

Sie können die Berichte in zwei OpenVAS-spezifischen Formaten und als HTML-Daten speichern. Auch der Export nach ASCII und XML ist möglich. Allerdings ist bislang kein direktes Schreiben der Berichtinformation in eine Datenbank möglich. In Sachen WLAN hat OpenVAS leider wenig zu bieten. In der aktuellen Version sind keine nennenswerten Skripte für die Analyse von WLAN-Komponenten im Netzwerk enthalten.

NVT-Feeds konfigurieren

Die NVTs sind so etwas wie das Herzstück der OpenVAS-Umgebung. Ihre Tests und deren Ergebnisse sind immer nur so gut wie die NVT-Ausstattung. Da fast täglich neue Skripte und Updates verfügbar sind, sollten Sie dafür sorgen, dass OpenVAS immer auf dem neuesten Stand ist. Hierfür stellen Ihnen die Entwickler den Feed-Service zur Verfügung. Mit seiner Unterstützung werden nur neue und veränderte Skripte heruntergeladen, zusammen mit den jeweiligen Signaturen (asc-Dateien) und einer Datei mit Prüfsummen (md5sums).

Der Synchronisationsprozess basiert auf der RSYNC-Technologie. Die Signaturen sind nur dann relevant, wenn Sie Ihren OpenVAS-Server dazu konfiguriert haben, nur signierte Skripte auszuführen. Um den Feed-Service nutzen zu können, benötigen Sie neben dem Plug-In-Modul, inklusive dem Skript *openvas-nvt-sync*, die Programme "rsync" und "md5sum". Um nun Ihre lokale NVT-Sammlung mithilfe des Feed-Services auf den neuesten Stand zu bringen, stellen Sie zunächst sicher, dass das Synchronisationsskript installiert ist. Sie finden es standardmäßig im Verzeichnis "/usr/local/ sbin/openvas-nvt-sync".

Prüfen Sie dabei insbesondere auch, ob die Variablen "NVT_DIR" und "FEED" die für Ihre Konfiguration korrekten Werte beinhalten. Als Nächstes rufen Sie das Synchronisationsskript mit # *openvas-nvt-sync* auf. Das Skript führt einen Datenabgleich mit dem angegebenen NVT-Feed-Service aus. Nach der Synchronisation werden die Prüfsummen aller synchronisierten Datei-

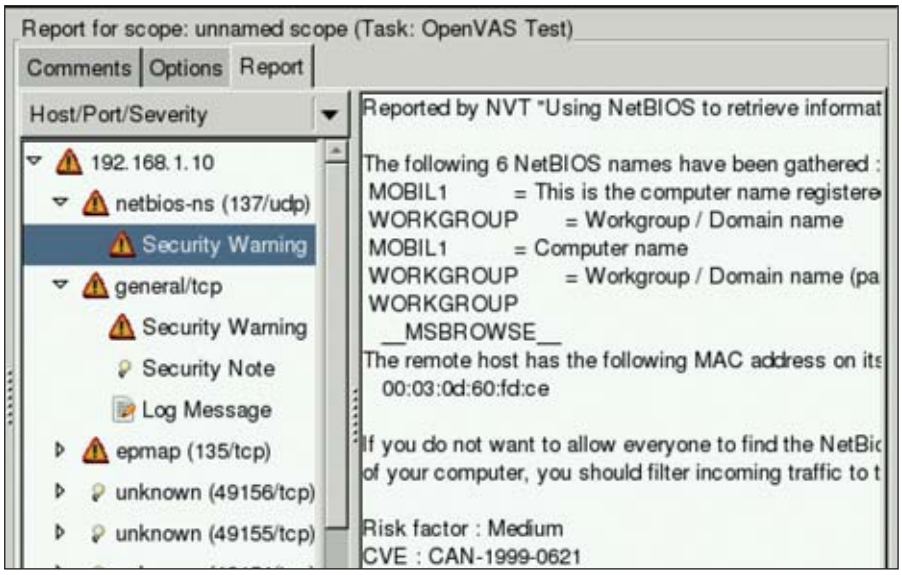


Bild 2: Ein Bericht im OpenVAS-Client präsentiert die Ergebnisse in übersichtlicher Form

en überprüft. Führen Sie abschließend einen Neustart des OpenVAS-Servers aus.

Security Scanning deluxe

Mit dem Greenbone Security Assistant (GSA), dem OpenVAS-Administrator und dem OpenVAS-Manager hat das Entwickler-Team drei vollständig neue Komponenten für das OpenVAS-System entwickelt. Dabei sticht der GSA besonders hervor, ein webbasiertes Tool, über das Sie alle wichtigen Aufgaben bei der Durchführung Ihrer Sicherheitschecks in Auftrag geben. Es handelt sich also um eine webbasierte Alternative zum OpenVAS-Client, die in einigen Bereichen sogar mehr zu bieten hat als der OpenVAS-Client.

Der GSA stellt Ihnen einen Webserver und damit eine webbasierte Schnittstelle zur Verfügung, über die alle wichtigen Aktionen für die Durchführung Ihrer Scans möglich sind. Der Webserver wurde mit libmicrohttpd [2] realisiert. Sie können Ihre bestehenden Scan-Profile von einem Desktop-Client in den GSA importieren und dort nutzen. Der vielleicht wichtigste Vorteil: Selbst technisch weniger versiertes Personal kann spezielle Prüfungen durchführen. Wie bei dem OpenVAS-Client können Sie mit wenigen Mausklicks PDF-, HTML- und XML-Exporte der Berichte erstellen. Eine weitere Besonderheit: Der GSA zeigt auf einfache Weise den Sicherheitsstatus und dessen Trend an.

Zum besseren Verständnis: Der OpenVAS-Manager ist die neue OMP-Schicht. Sie sitzt grundsätzlich zwischen Scanner und Client. Damit wird es beispielsweise ermöglicht, Ergebnisse schon während eines laufenden Scans einzusehen. Sie müssen also nicht, wie beim Client, warten, dass der Scan fertig ist. Der Administrator ist hingegen eine optionale Komponente. Damit können Sie Benutzer verwalten und beispielsweise auch den NVT-Feed aktualisieren. Der GSA ist das GUI für beide. Ein weiterer Vorteil des GSA: Sie müssen Benutzer nicht mehr an der Kommandozeile anlegen, sondern erledigen das bequem aus der GUI heraus. Für den Einsatz spricht außerdem, dass Sie Scans zeitlich steuern können. Auch der automatische Versand einer Mail ist möglich, wenn ein Scan den Status ändert.

GSA in der Praxis

Der GSA bietet all die Funktionen, die Sie auch im OpenVAS-Client finden – und mehr. Die Funktionen des Bereichs Scan-Management dienen in erster Linie dem Erstellen und dem Verwalten von Scan-Aufträgen. Beim Zugriff auf den GSA präsentiert Ihnen das Tool standardmäßig die Task-Übersicht. Zu jeder Aufgabe werden die Bezeichnung, der Status, die Berichte, die Threads, die Trends und verfügbare Aktionen aufgeführt. Um eine erste Aufgabe anzulegen, folgen Sie dem Link "New Task" und spezifizieren in dem zugehörigen Dialog die Scan-Eigenschaften. Wenn Sie im Bereich "Configuration" dem Link "Scan Configs" folgen, landen Sie in einem umfangreichen Formular, das Ihnen das Erstellen neuer Scan-Konfigurationen erlaubt. Auch der Import von bestehenden Konfigurationen ist möglich, solange diese XML-basiert sind.

Der GSA hat zwei weitere Besonderheiten zu bieten: Mit "Escalator" wählen Sie einen Trigger aus, der bei bestimmten Ereignissen ausgelöst wird. Außerdem erlaubt das Auswahlmenü "Schedule" die Wahl von Zeitplänen für die zeitliche Steuerung des Scan-Vorgangs. Sie müssen ebenfalls zuerst angelegt werden. Ein wesentliches Element eines anspruchsvollen Schwachstellenmanagements ist

Bild 3: Mit dem Greenbone Security Assistent macht Security-Scannen richtig Spaß. Der GSA bietet deutlich mehr Komfort als der OpenVAS-Client und zusätzliche Funktionen.

Bestellen Sie jetzt

das IT-Administrator

Sonderheft II/2010!

180 Seiten Praxis-Know-how
rund um das Thema

Active Directory

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft II/2010 für € 24,90. Nichtabonnenten zahlen € 29,90. IT-Administrator All-Inclusive Abonnenten "zahlen" für Sonderhefte nur € 19,90 - diese sind im Abonnement dann automatisch enthalten. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.*

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

---

administrator
Das Magazin für professionelle System- und Netzwerkadministration

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

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

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0211

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

Scan Configs

Name	Families		NVTs		Actions
	Total	Trend	Total	Trend	
Full and fast (All NVT's; optimized by using previously collected information.)	45		17338		
Full and fast ultimate (All NVT's including those that can stop services/hosts; optimized by using previously collected information.)	45		17338		
Full and very deep (All NVT's; don't trust previously collected information; slow.)	45		17338		
Full and very deep ultimate (All NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	45		17338		
IT-Grundschutz Scan	1		2		
empty (Empty and static configuration template.)	0		0		

Bild 4: Die Übersicht der Scan-Konfiguration im Greenbone Security Assistant

das Erstellen und Verwalten von Notizen. So ergänzen Sie die Detailinformationen um wichtige Zusatzinformationen. Der GSA stellt Ihnen hierfür eine leistungsfähige Notizfunktion zur Verfügung. Das Besondere daran: Ihre Anmerkungen können auch in die Berichtexporte aufgenommen werden.

Der Bereich "Configuration" dient der Konfiguration der Scans. Hier bestimmen Sie, welche NVTs ausgeführt, welche Ziele ins Visier genommen und welche Zugangsdaten für lokale Tests verwendet werden. Außerdem können Sie hier "Agents" (Drittanwendungen) sowie Warnungskriterien definieren und zeitliche Steuerungen anlegen.

Windows-Systeme scannen

OpenVAS wird häufig in heterogenen Umgebungen zum Scannen von Windows-Hosts verwendet. Auch bei Windows-Systemen ist ein Scannen des Innenlebens, genauer der Windows-Registrierungsdatenbank, möglich. Diesen Zugriff haben in der Regel nur Windows-Systemadministratoren. Aber mit einigen Eingriffen in ein Windows-System lässt sich auch dies mittels OpenVAS analysieren. Dazu sind allerdings auch Eingriffe in die Windows-Registrierungsdatenbank erforderlich.

Zunächst sind eine ganze Reihe von Anpassungen aufseiten des Windows-Systems erforderlich. Als Erstes erzeugen Sie eine neue Benutzergruppe, die Sie beispielsweise als OpenVAS-Test bezeichnen. Als Nächstes legen Sie in dieser Benutzergruppe einen OpenVAS-User an, den Sie beispielsweise einfach als OpenVAS bezeichnen. Damit OpenVAS Remote-Zugriff auf das Windows-System erlangen kann, müssen Sie einen Registrierungsschlüssel anpassen. Der Remote-Zugriff wird über den Schlüssel "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg" aktiviert.

Dieser Schlüssel muss nun angepasst werden, damit der zuvor erzeugte OpenVAS-Benutzer auf das System zugreifen kann. Dazu führen Sie folgende Schritte aus:

1. Zunächst öffnen Sie mit dem Registrierungseditor den Schlüssel "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control".
2. Diesen markieren Sie, führen dann den Befehl "Neu / Schlüssel" aus und bezeichnen diesen als "SecurePipeServers". Als Typ verwenden Sie "REG_SZ".
3. Dann öffnen Sie den neu erzeugten Schlüssel "SecurePipeServers" und erzeugen einen neuen Unterschlüssel "winreg".
4. Außerdem erzeugen Sie eine neue Zeichenfolge, bezeichnen diese mit "Description" und geben als Wert "REG_SZ" an.
5. Abschließend modifizieren Sie die Zeichenfolge "Description" und weisen ihr den Wert "Registrierungsserver" zu.

Als Nächstes gilt es, die Berechtigungen für die Zusammenarbeit mit OpenVAS zu setzen. Auch hierfür nutzen Sie den Registrierungseditor. Zunächst öffnen Sie den oben erzeugten Schlüssel und führen dann den Befehl "Bearbeiten / Berechtigungen" aus. Im Dialog "Berechtigungen für winreg" klicken Sie auf "Erweitert", um die erweiterten Berechtigungen zu öffnen. Dann klicken Sie auf "Hinzufügen", um den OpenVAS-Benutzer hinzuzufügen und bestätigen mit "OK". Auf dem Register "Berechtigungen" bearbeiten Sie die Einstellungen des OpenVAS-Benutzers "OpenVAS", der zumindest Leserechte benötigt. Abschließend speichern Sie die Einstellungen.

Als Nächstes müssen Sie nur noch die Einstellungen des OpenVAS-Clients anpassen. Dort öffnen Sie das Register "Credentials" und navigieren dort zu den Windows-Credentials-Einstellungen. Unter "SMB account" und "SMB password" geben Sie die oben verwendete Benutzerkennung und das Passwort des erzeugten OpenVAS-Benutzers ein. Nicht zwingend ist die Angabe der SMB-Domain. Bei der nächsten Ausführung von Test-Skripten, die Zugriff auf die Windows-Registry benötigen, kann OpenVAS auch auf diese zugreifen und die relevanten Informationen auslesen.

Link-Codes

[1] Download OpenVAS
B2P41

[2] InterGNU libmicrohttpd
B2P42

[3] Interview mit Jan-Oliver Wagner, Kopf des OpenVAS-Teams
B2P43

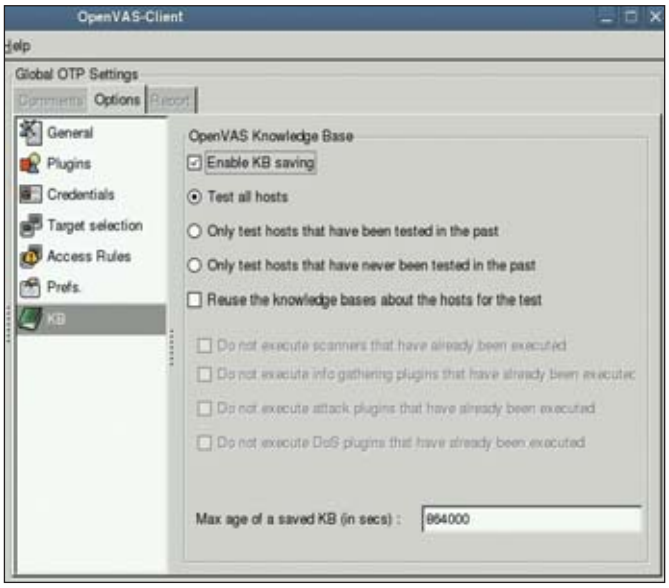


Bild 5: Die Knowledge Base muss zunächst aktiviert und konfiguriert werden

Die Knowledge Base

Durch die Kategorisierung der Plug-Ins wird eine strenge Aufgabentrennung in OpenVAS erreicht. Die Testergebnisse landen allesamt in der Knowledge Base. Die Ergebnisse einzelner Hosts werden in einem speziellen Knowledge Base-Verzeichnis abgelegt.

Hat der Benutzer User beispielsweise Host 192.168.0.1 gescannt, so findet er die zugehörigen Knowledge Base-Einträge bei einer Standardinstallation unter /var/lib/openvas/users/User/kbs/192.168.0.1. Es handelt sich um eine textbasierte Sammlung der durchgeführten Tests. Die Inhalte sind natürlich von den durchgeführten Tests abhängig. Während manche Zeilen rein informative Daten enthalten, beinhalten andere Scan-Einstellungen oder Details zu Reaktionen auf Scan- und Testvorgänge. Der Knowledge Base lässt sich exakt entnehmen, welche Daten beispielsweise an einen Dienst gesendet wurden. Auch der Verwundbarkeitstyp lässt sich ihr entnehmen. Während der Tests wird übrigens eine temporäre Datei erzeugt, in der die aktuellen Ergebnisse landen. Es handelt sich um eine Datei im NBE-Format, die standardmäßig im TMP-Verzeichnis liegt. Nachdem die Tests abgeschlossen sind, können Sie die Daten wie oben beschrieben in eines der vielen Exportformate konvertieren.

Damit Sie in den Genuss der Knowledge Base-Daten gelangen, müssen Sie die Knowledge Base zunächst aktivieren. Dazu öffnen Sie in den Scan-Einstellungen das Register "KB" und aktivieren die Wissensbasis, indem Sie das Kontrollkästchen "Enable KB saving" anklicken. Die Konfiguration der Knowledge Base erfolgt über den OpenVAS-Client. Zunächst sollten Sie sicherstellen, dass die Option "Enable KB saving" aktiviert ist. Über die folgenden Schalter steuern Sie exakt, welche Hosts unter die Lupe genommen werden und ob die Inhalte der Knowledge Base wieder verwendet werden sollen oder nicht. Wenn Sie den OpenVAS-Client benutzen, so sollten Sie die Option "Test all hosts" aktivieren, denn so werden alle Systeme, die Sie als Ziele unter "Target Selection" angegeben haben, untersucht. Alternativ können Sie bei diesem Client die Option "Only test hosts that have been tested in the past" verwenden, um nur bereits getestete Hosts zu testen, oder die Option "Only test hosts that have never been tested in the past", um bislang noch nicht getestete Systeme zu untersuchen.

Der gezielte Einsatz dieser Schalter ist beispielsweise sinnvoll, wenn Sie nach Änderungen einer Subnetz-Umgebung lediglich neu hinzugekommene Systeme untersuchen wollen. Sinnvoll ist deren Verwendung auch, wenn Sie bei bereits gescannten Umgebungen Sicherheitslücken durch das Einspielen von Patches et cetera geschlossen haben und nun überprüfen wollen, ob sich deren Einsatz positiv auf die Ergebnisse auswirkt. Auch bei der Verwendung von DHCP im lokalen Netzwerk kann es sinnvoll sein, Tests beispielsweise bei allen Hosts durchzuführen.

Fazit

OpenVAS ist zweifelsohne ein würdiger Nessus-Nachfolger. Insbesondere das GSA macht die Durchführung, das Verwalten und Auswerten von Tests ausgesprochen benutzerfreundlich. Anwender, denen das Tempo der Weiterentwicklung nicht schnell genug geht, sind herzlich aufgerufen, sich einzubringen. Insbesondere bei der NVT-Entwicklung dürfte das OpenVAS für jede Hilfe dankbar sein. *(jp)*

Quelle: electriceye - Fotolia.com

Bladeserver-Management mit HP Virtual Connect (1)

Starthilfe im Serverschrank

von Betram Wöhrmann

In unserem Einkaufsführer im Januar haben wir Ihnen aufgezeigt, welche technischen Möglichkeiten Sie sich mit dem Einsatz der Bladeserver-Technologie ins Rechenzentrum holen. Doch birgt diese Technik auch Fallstricke. In unserer zweiteiligen Workshopserie zeigen wir Ihnen auf, wie Sie ein solches System verwalten und welche erweiterten Optionen Ihnen hierfür der HP Virtual Connect Enterprise Manager bietet.

HP hat bei seinen Blade-Enclosures eine Technologie mit Namen Virtual Connect etabliert. Diese Technologie ist eine Virtualisierungsschicht, die sich zwischen dem Bladeserver und den physischen Netzwerk- beziehungsweise Fibre Channel-Komponenten einfügt. Sie haben damit die Option, den Servern virtuelle MAC-Adressen oder World Wide Names (WWNs) zu geben und eine Entkopplung zwischen der Rechenzentrums-Infrastruktur und dem Server zu erreichen. Die grundlegende Konfiguration erfolgt erst nach der vollständigen Inbetriebnahme des Enclosures selbst. Alle hier gezeigten Informationen basieren auf der größeren Variante des Enclosures, dem HP Bladesystem c7000 Enclosure. HP bietet noch eine kleinere Variante an, das HP Bladesystem c3000 Enclosure. Diese Variante hat geringere Ausbaumöglichkeiten, was die Anzahl der Server beziehungsweise der Verbindungen nach außen angeht. Sie eignet sich besonders gut für kleinere Außenstandorte.

Inbetriebnahme

Zur Inbetriebnahme Ihres neuen Enclosures müssen Sie zunächst einmal die IP-Adresse konfigurieren und die Management-Module mit dem Netzwerk verbinden. Alle nachfolgenden Arbeiten können Sie dann mit dem Webbrowser durchführen. Die Oberfläche gliedert sich in mehrere Bereiche: Im linken Teil finden Sie eine Übersicht aller Funktionen. Oben in der Kopfzeile können Sie Funktionen über die Menüleiste aufrufen. In dem Fenster unterhalb erfolgt die Anzeige der aufgerufenen Option. Die linke Spalte gliedert sich in mehrere Abschnitte. Im oberen Bereich erfolgen die Einstellungen für das Enclosure selbst und die IP-Konfiguration aller managebaren Komponenten. Darunter werden die Onboard Administrator Module (OA) administriert. Das ist die Bezeichnung des Managementinterfaces. Es folgen die vorhandenen Server, die verwaltbaren I/O-Komponenten, eine Übersicht über den Stromverbrauch und das thermische Verhalten des Systems. Das User-Management ist der nächste Punkt und anschließend die Anzeige des integrierten Management-Displays. Der letzte Auswahlpunkt in diesem Bereich ist der Link zum Virtual Connect-Manager. Auf diese Technologie werden wir im nächsten Teil dieser Artikelserie eingehen. Dabei wird es sowohl um die Technik als solches als auch um die Verwaltung dieser Funktion gehen.

Bevor Sie für die weiteren Arbeiten auf das Enclosure mit dem Webbrowser zugreifen können, müssen Sie nach der hardwareseitigen Inbetriebnahme über das

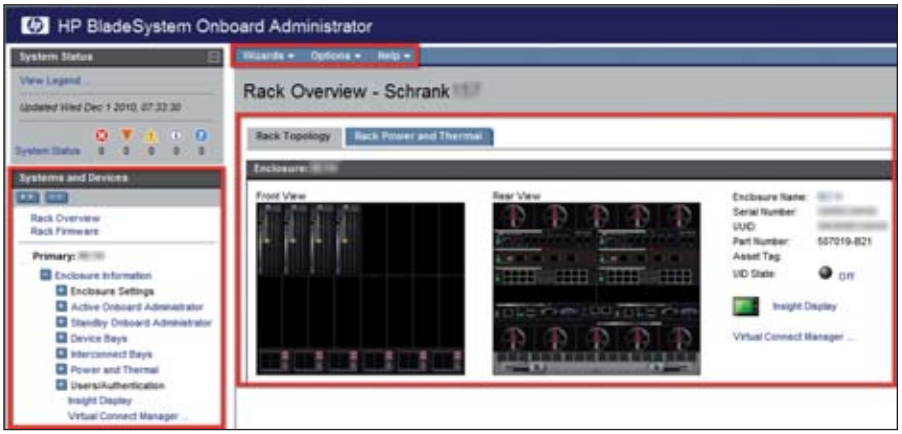


Bild 1: Managementoberfläche des Blade-Systems HP Enclosure c7000

Bild 2: Das Enclosure Insight Display in der Managementoberfläche

Insight Display an der Front die IP-Konfiguration einstellen. Dort können Sie auch die weiteren Einstellungen vornehmen, aber bequemes und effizientes Arbeiten ist etwas anderes. Normalerweise wird Ihnen hier der Status des Chassis angezeigt. Die Anzeige des Displays können Sie sich auch im Browser anzeigen lassen oder beispielsweise einem Techniker vor Ort eine Nachricht dorthin übermitteln.

Grundeinstellungen mit oder ohne Wizard

Bevor wir nun näher auf die Konfiguration des Enclosures eingehen, möchten wir Sie noch darauf hinweisen, dass es auch Wizards gibt, die Sie bei der Konfiguration der Komponenten unterstützen. In diesem Workshop gehen wir dennoch auf die einzelnen Konfigurationspunkte ein, die Sie auch im Wizard wiederfinden. Kommen wir nun zur weiteren Konfiguration des Chassis. Grundsätzlich führen Sie alle weiteren Arbeiten mit dem Browser durch. Erweitern Sie den Punkt "Enclosure Settings", um die Konfigurationspunkte sehen zu können. Dort passen Sie zu Beginn die Grundeinstellungen an, die Menüpunkte sind dabei selbsterklärend – von der Benachrichtigung bei auftretenden Fehlern über die Einschaltreihenfolge bis zur Einstellung der Zeit beziehungsweise eines Timeservers. Bei den "Enclosure IP-Settings" finden Sie zudem eine wichtige Einstellung, falls Sie mit zwei Managementmodulen arbeiten möchten: Es ist dort möglich, jedem Management-Modul eine eigene IP-Adresse zu geben. Die bessere Wahl ist jedoch die Aktivierung des Punktes "Enclosure IP Mode". Dieser bewirkt, dass Sie immer über dieselbe IP-Adresse auf das Gerät zugreifen können, egal welches Management-Modul aktiv ist. Die IP-Adresse zieht beim Umschalten also einfach mit um. So müssen Ihnen nicht beide IP-Adressen bekannt sein, um sich auf einem Enclosure anzumelden. Sie werden direkt auf das aktive Modul geleitet und können so Ihre Arbeiten durchführen.

Unter dem Punkt "Network Access" legen Sie fest, auf welche Art und Weise der Zugriff erfolgen darf. Beachten Sie hier die Sicherheitsrichtlinien Ihres Unternehmens. Es folgt die Einstellung des Verhaltens bei einem Verlust der Netzwerkverbindung sowie die Konfiguration der SNMP-Einstellungen. Hinter der Auswahl "Bay IP Addressing" verbirgt sich die Versorgung aller aktiven Komponenten mit IP-Adressen, um sie administrieren zu können. Hierzu eine kurze Erläuterung, wie der Zugriff auf die einzelnen Komponenten des Enclosures erfolgt: Über die Management-Module werden auch alle anderen aktiven Komponenten administriert. Damit ein Zugriff auf diese Komponenten erfolgen kann, müssen Sie den Servern und aktiven Netzwerk- beziehungsweise Fibre Channel-Komponenten Management-IP-Adressen mitgeben. Dies erfolgt unter dem Punkt "Bay IP Addressing". Sollten Sie hier keine Einstellungen vornehmen, könnten Sie nicht auf die Server per iLO (Remotezugriffskonsole bei HP-Servern) zugreifen.

Über den Punkt "Configuration Scripts" sichern Sie die Konfiguration eines Enclosures beziehungsweise spielen diese wieder ein. Hier besteht die Möglichkeit, die Gesamtkonfiguration zu exportieren, wenn Sie etwa einmal dem HP-Support Informationen liefern müssen oder wenn Sie ein weiteres Enclosure konfigurieren wollen. Dazu kann das erzeugte File mit den neuen Parametern wie der neuen IP-Adresse angepasst und eingespielt werden. Über "Active to Standby" kann der aktive Management-Kontroller gewechselt werden. Dies können Sie auch dadurch provozieren, indem Sie den aktiven Kontroller hardwareseitig temporär aus dem Enclosure entfernen. Der Punkt "Firmware Update" unter dem aktiven Onboard-Controller macht genau das, was er aussagt. In dem zugehörigen Fenster wird das passende File hinterlegt und das Firmware-Update auf beiden Management-Modulen durchgeführt. Den Servern macht das nichts aus, sie laufen ohne Unterbrechung weiter. Bedenken Sie aber, dass der Firmware-Releasestand der Server von der Onboard Administration-Firmware unterstützt werden muss. Die richtige Reihenfolge bei solchen Arbeiten beginnt mit dem Update der Treiber auf den Servern, dann folgt die Firmware der Server. Als Nächstes aktualisieren Sie den OA und abschließend folgt die Firmware der aktiven Komponenten für die externe Anbindung der Server (siehe Kasten "Patchreihenfolge").

Neue Server hinzufügen

Sollen neue Server in ein vorhandenes Enclosure verbaut werden, das mit Virtual Connect-Modulen ausgestattet ist, ist ein weiterer Arbeitsschritt nötig. Vor der Aktualisierung der Server-Firmware ist in jedem Fall das Serverprofil anzuhängen. Dazu kopieren Sie ein vorhandenes oder erstellen ein neues Profil und binden dieses an den Steckplatz des neuen Servers. In dem Profil wird festgelegt, wie der Server mit der Außenwelt verbunden wird. Sollten Sie sich nicht an diese Vorgehensweise halten, kann es zu Verbindungsproblemen kommen. Weiter unten sehen Sie die Anzeige aller eingebauten Server und der Verbindungsmodule. Neben der Darstellung der Komponenten und der Ausstattung findet sich hier auch der Health-Status des Blades. Die von HP bekannte Integrated Lights-Out-Funktion (iLO) schließt sich in einem separaten Punkt an.

Eine andere hilfreiche Funktion verbirgt sich hinter dem Punkt "Port Mapping" (Bild 3). Sie zeigt Ihnen, wo die Anschlüsse des einzelnen Servers in das I/O-Interface münden. Letztendlich bestimmt die Hardware-Schaltung im Enclosure selbst, an welchem Bay die Anschlüsse der einzelnen Server anliegen. Nutzen Sie hier die Anbindungen, die sich auf dem Motherboard des Blades befinden, werden nur Verbindungsmodule in Bay 1 und Bay 2 benötigt. Die Anschlüsse der ersten Erweiterungskarte (im HP Terminus Mezzanine-Karte) enden in Bay 3 und Bay 4. Wird bei Servern mit doppelter Baugröße eine weitere Erweiterungskarte eingesetzt, enden die Ports in Bay 4 bis Bay 6, je nach verwendeter Karte. Identische Kartentypen müssen zwingend immer im identischen Slot verbaut werden – so etwa die Fibre Channel-Karte immer im ersten Erweiterungsslot. Damit enden alle Fibre Channel-Anschlüsse in Bay 2 und Bay 3. Das Enclosure zeigt Ihnen aber auch eine Fehlermeldung an, wenn die Konfiguration des Servers nicht zur Konfiguration des Chassis passt.

Beachten Sie, dass hier nicht der Ausgangsport angezeigt wird, sondern nur der interne Eingangsport des Interconnect-Moduls. Die Zuweisung zu den Ausgangsports ist nur ersichtlich, wenn Sie mit Passthru-Modulen arbeiten. Mit der Maus können Sie den Anschluss aktivieren/deaktivieren und sehen so, wo der zugehörige Port an die zentrale Infrastruktur angeschlossen werden muss.

Unter dem Punkt "Power and Thermal" finden Sie das Temperatur- und Wärmemanagement. Hier lässt sich genau erkennen, ob es einen Temperatur-Hotspot gibt. Weiterhin können Sie hier das Verhalten der Netzteile festlegen, etwa mit welcher Ausfallsicherheit gearbeitet werden soll. Sie finden hier außerdem eine detaillierte Anzeige des Verbrauchs für jede Komponente. Selbstverständlich gilt das auch für die Kühlleistung. Auch hier wird nur die Leistung abgerufen, die wirklich von allen verbauten Komponenten benötigt wird. Dabei gibt es verständlicherweise eine Ausnahme. Kommt es zu Problemen mit den Managementmodulen, wird die Kühlleistung auf das Maximum hochgefahren, um eine Überhitzung des Systems zu verhindern, denn die Module steuern diese Funktion.

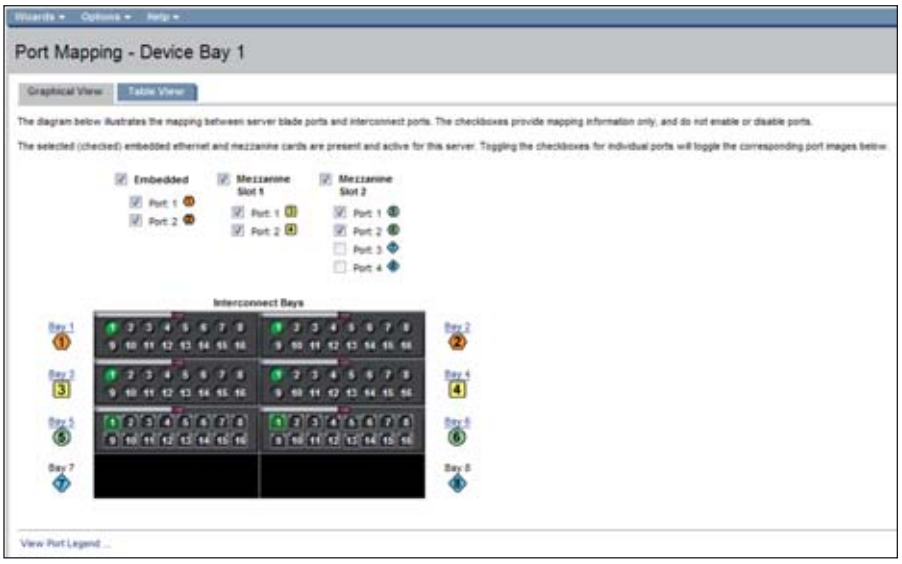


Bild 3: Das Portmapping des Servers verrät, wo die Server in das I/O-Interface münden

Möchten Sie ein DVD/CD-Laufwerk lokal an das Enclosure anschließen, um Medien mit den verbauten Servern zu nutzen, wählen Sie den zugehörigen Menüpunkt "DVD Drive" aus. Hier können Sie das Laufwerk zuweisen und so zentral installieren oder patchen. Beachten Sie aber, dass HP Empfehlungen für die maximale Anzahl von gleichzeitigen Aktionen abgibt. Halten Sie sich daran, sonst kann es passieren, dass die gewünschten Aktionen nicht einwandfrei ablaufen.

Ein weiterer Punkt für die Konfiguration des Netzwerkes verbirgt sich hinter "VLAN Configuration". Dort lassen sich für alle aktiven Komponenten unterschiedliche VLANs konfigurieren. HP empfiehlt für eine einwandfreie Funktion, dass das Managementinterface aller Komponenten im selben VLAN liegt und so ist das Chassis auch konfiguriert. Ist das bei Ihnen nicht der Fall, dann können Sie hier die entsprechenden Konfigurationsanpassungen vornehmen. Definieren Sie hier Ihre VLANs und benennen Sie diese entsprechend, um sie anschließend mit den passenden Einschüben zu verbinden. Auch hier müssen Sie beachten: Das Mapping erfolgt nicht mit der einzelnen Komponente wie dem Server oder den Interconnect-Modulen, sondern über den Einschub.

Nutzerverwaltung und Zugriffe einrichten

Einer der letzten Punkte ist die Einrichtung der User, die auf das Enclosure und deren Komponenten zugreifen sollen. Sie können nicht nur lokale User anlegen, es kann vielmehr auch eine Verbindung an ein Active Directory erfolgen. Die Passwortsicherheit konfigurieren Sie hier ebenso wie eine Übersicht der derzeit angemeldeten Anwender. Nennen Sie größere Umgebungen Ihr Eigen, besteht auch die Option, mehrere Enclosures zentral über den HP Systems Insight Manager (SIM) zusammenzufassen. Dies wird ebenfalls an dieser Stelle eingerichtet. Als Letz-

Patchreihenfolge

1. Treiber im Betriebssystem
2. Firmware auf dem Server
3. Onboard Administrator-Enclosure
4. Interconnect-Module

tes finden Sie auf der linken Seite noch einen Link für den Aufruf des Virtual Connect-Managers, wenn Sie entsprechende Module verbaut haben, dazu aber mehr im nächsten Teil unserer Serie.

Konnte früher nur remote auf die Chassis über das Netzwerk zugegriffen werden, so besteht seit einiger Zeit die Option, an das Management-Modul einen Monitor nebst Maus und Tastatur anzuschließen. Über den integrierten KVM-Switch können Sie dann in gewohnter Manier auf die einzelnen Server gehen und an diesen arbeiten. Ein Anschluss für eine serielle Verbindung ist ebenfalls noch vorhanden. Zur Arbeit über die Kommandozeile kann dieser Weg gewählt werden. Nutzen Sie am besten die Zugriffsmöglichkeit, die Ihnen behagt und die die Sicherheitsrichtlinien in Ihrem Unternehmen zulassen. Sollte es erwünscht sein, können Sie auch eine Blacklist für den Zugriff auf die Hardware pflegen. Schränken Sie den Zugriff nicht an zu vielen Stellen ein, sonst haben Sie bei Zugriffsproblemen keine leichte Fehlersuche.

Greifen Sie per Browser auf ein Enclosure zu, so können Sie sich an diesem selbstverständlich anmelden. Sind die Systeme aber in den HP SIM eingebunden, können Sie alle Chassis sehen und unterschiedliche Enclosures in einer Oberfläche administrieren, ohne sich immer wieder anmelden zu müssen. Kommen kleinere Umgebungen zum Einsatz, besteht eine weitere Möglichkeit, einen ähnlichen Effekt zu erreichen. Über einen Connector zwischen den Management-Modulen können Sie Chassis direkt miteinander verbinden. Melden Sie sich dann auf einem Enclosure dieses Verbundes an, haben Sie die Option, die Anmeldung gleichzeitig an mehrere Systeme zu senden. Für diese Option gelten aber einige Bedingungen: Der genutzte User sollte identische Rechte auf allen Enclosures haben. Dabei ist es egal, ob er lokal angelegt worden oder in einem Active-Directory beheimatet ist. Auch ist die Anzahl von kaskadierbaren Systemen begrenzt. Es können bis zu sechs Enclosures in einem Verbund zusammengefasst werden.

Fazit

Grundsätzlich gibt es keinen Grund, Bedenken in Bezug auf den Einsatz von Bladeservern zu haben. So haben sich beispielsweise die Einsatzszenarien durch Storage- und Tape-Blades stark erweitert. Zudem ist HP den letzten logischen Schritt gegangen mit der Option, dass PCI-X oder PCI-e Karten mit Bladeservern genutzt werden können. Dies war zuvor meist ein K.-o.-Kriterium für den Einsatz von Bladesystemen. Auf den Einsatz der unterschiedlichen externen Verbindungsoptionen möchten wir an dieser Stelle nicht tiefer eingehen. Werden etwa Passthru-Module genutzt, haben Sie eine Verkabelung vergleichbar zu klassischen Servern. Sie benötigen in dem Fall nur die entsprechende Menge an Ports in Ihrem Rechenzentrum. Setzen Sie Switche ein, können Sie diese in gewohnter Manier administrieren, so wie es der Hersteller empfiehlt. Eine Ausnahme bietet hier die entsprechende Virtual Connect-Technologie, wie Sie im zweiten Teil unserer Serie erfahren. *(dr)*

Bild 4: Die Verteilung der Kühlleistung in den vier Zonen

Erfolgsfaktoren bei Planung und Einführung eines Monitoring

Allzeit klare Sicht

von Sascha Giebelhausen

Quelle: Sveta - Fotolia.com

Im Idealfall überprüft und überwacht der Administrator seine IT-Umgebung ständig und permanent. Realistisch betrachtet findet sich wohl kaum ein Administrator, der auch nur ein Eventlog vor dem ersten Kaffee geprüft hat. Anomalien, die noch keine Einschränkungen im Netzwerk verursachen, haben also genug Zeit, kritisch zu werden. Und wenn es dann soweit ist, heißt es reagieren statt agieren. Besser ist es da, wenn eine konsequente und proaktive Monitoringstruktur Fehler frühzeitig erkennt und dem Admin Zeit für sein Frühstücksgetränk lässt. Dieser Artikel zeigt auf, wie das Monitoring geplant, welche Komponenten überwacht und was bei der Tool-Auswahl beachtet werden sollte.

Stellen Sie sich als IT-Verantwortlicher die Frage "Welchen Stellenwert hat das Monitoring für mich oder meine IT- und Telekommunikations-Infrastruktur?", so werden Sie sicher mit mindestens einem der vier nachstehenden Sätze antworten:

1. Die Kunden/Mitarbeiter rufen schon an, wenn etwas nicht funktioniert.
2. Was bringt mir ein Monitoring, das nur bereits aufgetretene Fehler reportet?
3. Wir können SLAs auch mit einem Monitoring nicht einhalten.
4. Wir hatten mal eins, aber irgendwann war mein Postfach mit Fehlern zugespammt!

Die IT-Abteilung eines Unternehmens sollte immer alles daran setzen, die Probleme zu lösen, bevor sie von den Kollegen wahrgenommen werden. Das gelingt natürlich nur, wenn das Monitoring auf allen eingesetzten, geschäftskritischen oder -unterstützenden Technologien erfolgt. Dabei ist jedoch die Faustregel zu berücksichtigen, dass die Priorität immer auf den für das Kerngeschäft und den Geschäftsprozessen benötigten Technologien liegt und das Tagesgeschäft auch nicht vernachlässigt werden darf. Zudem lässt sich über ein Monitoring gegebenenfalls auch ein Virenbefall oder Angriffsversuche auf beispielsweise das Active Directory frühzeitig erkennen.

Ein einfaches Beispiel: Bei jedem Monitoring sollte auf allen Domänencontrollern geprüft werden, wie oft das "Ereignis 675" seit der letzten Überprüfung aufgetaucht ist. Dieses Ereignis wird automatisch im Ereignisprotokoll auf dem jeweiligen Anmeldeserver (der erste erreichbare Domänencontroller) mitgeschrieben, wenn eine Benutzeranmeldung an der Domäne mit einem falschen Kennwort fehlschlägt. Dieses Ereignis wird bei Schadcode mit Brute Force-Attacken häufig sogar mehrmals pro Sekunde im Ereignisprotokoll niedergeschrieben und kann durch die Überlastung der Domänencontroller ganze Informations- und Telekommunikations-Infrastrukturen lahmlegen (im Übrigen ist diese Event-ID auch ein Zeichen für Conficker). Dies bedeutet jedoch nicht, dass der Einkauf den Virenschutz einfach durch das Monitoring ersetzt und damit gegebenenfalls Lizenzen spart. Das Monitoring ist als eine weitere Schutztechnologie zu sehen und dient lediglich zur Erhöhung der Sicherheit in IT-Infrastrukturen.

Einfluss von Kernprozessen auf den Monitoring-Zyklus

Der Monitoring-Zyklus orientiert sich in erster Linie an den Kernprozessen Ihres Unternehmens. Als Grundlage dafür dienen in den meisten Fällen Notfallvorsorgekonzepte oder Service Level Agreements (SLAs), in denen die Wichtigkeit der (IT-gestützten) Prozesse festgehalten werden. Je nach Ausrichtung und Kernkompetenz des Unternehmens kann es mehr oder auch weniger auf die jeweiligen Technologien angewiesen sein.

So ist zum Beispiel eine reine Büroumgebung häufig auf die klassischen Infrastrukturdienste angewiesen: Verzeichnisdienste (Active Directory, Novell), E-Mail (Exchange, Notes et cetera), Terminalserver, Storage-Systeme, Datenbankserver oder auch die IP-basierte Telefonanlage. Daher muss die Funktionalität und Verfügbarkeit dieser Technologien permanent gewährleistet werden. In kritischen Infrastrukturen, die häufig bei produzierenden Unternehmen (allen voran Energieversorgern) zu finden sind, ist es häufig so, dass die klassischen Büroapplikationen und -dienste nicht existieren oder für den Betrieb nicht zwingend erforderlich sind.

Grundsätzlich gilt, dass die wichtigsten Technologien für die Erfüllung des Kernprozesses in das Monitoring-Konzept einfließen müssen. Alle weiteren Prozesse sollten Sie natürlich ebenfalls zyklisch prüfen, dies kann jedoch auch in einem größeren Intervall erfolgen. Dabei sollten natürlich auch nachgelagerte Dienste wie Virenschutz, Verzeichnisdienste oder die Netzwerkinfrastruktur überwacht werden.

Zu überwachende Komponenten und Dienste

Zeitnahe Information über alle wichtigen Vorkommnisse und Fehler in Ihrer Infrastruktur sind genauso wichtig wie das Melden "nur" relevanter Fehler. Bei Fehlern oder außerplanmäßigen Änderungen können beispielsweise durch eine Alarmierung alle notwendigen Maßnahmen für die Beseitigung/Behebung eingeleitet und in schriftlicher Form dokumentiert werden. Zu diesen Informationen können die folgenden Kriterien gehören:

- Ebene 1 mit Netzwerkkomponenten (Firewalls und Switches): Fehler und Warnungen in Eventlogs, Netzwerkauslastung, Neue Netzwerkgeräte
- Ebene 2 mit Serverkomponenten (Fileserver, Storage, Bandlaufwerke): Freier Speicherplatz auf Storage-Systemen/Fileservern, Überprüfung der Freigabesicherheit/NTFS-Sicherheit auf Konformität, Windows (Server und Clients), fehlerhafte Hardware-Komponenten von IT-Systemen
- Ebene 3 mit Diensten: Virenschutz (Status der Verteilung von Virensignaturen, Übersicht über Virenvorfälle innerhalb einer Umgebung), Verzeichnisdienst (Fehler und Warnungen in Eventlogs, Fehlgeschlagene Anmeldungen am Verzeichnisdienst, Computer-/Benutzerkonto deaktiviert, Konto existiert nicht, Benutzerkonto gesperrt), Aufzeigen von Fehlern innerhalb des Verzeichnisdienstes, neue Systeme, Änderungen an Gruppenmitgliedschaften, Verstöße gegen Namenskonventionen, Datensicherung (Übersicht des Status von Backupaufträgen, Tapestatus, freier Speicher, Laufzeit), Patchmanagement (Systeme mit fehlerhaften Updateinstallationen, Status der Verteilung von Sicherheitsupdates, Systeme ohne installierte Updates), neue Systeme (Lizenzstatus aller eingesetzten Technologien/Anwendungen, Updates und neue Versionen für Technologien/Anwendungen)

Manuelles vs. automatisches Monitoring

Viele Technologien bringen entsprechende Tools zur Diagnose mit, nur müssen die daraus resultierenden Meldungen auch entsprechend ausgewertet und notwendige Maßnahmen eingeleitet werden. Dies lässt sich durch einen Mitarbeiter, einen externen Dienstleister oder über eine sogenannte Monitoring-Lösung bewerkstelligen. Hier gibt es jedoch gravierende Unterschiede, denn falls das Monitoring in Ihrer Umgebung noch manuell durchgeführt wird, so haben sie nur zwei kleine, aber sehr gravierende Nachteile:

1. Keine permanente Überwachung
2. Fehlende Alarmierung bei Fehlern

Je nach Aufbau der Geschäftsprozesse können diese Nachteile gesamte Produktionsstraßen, Kraftwerke oder Büronetzwerke zum Erliegen bringen. Folge sind dann entsprechende Umsatzeinbußen oder Probleme beim Einhalten von Lieferzeiten. Saftige Vertragsstrafen können das Resultat sein. Die einzig wahre Lösung ist eine Software, die das permanente Monitoring mit Alarmierung übernimmt. Dies erlaubt, die personellen Ressourcen auch an den Stellen einsetzen können, wo sie wirklich gebraucht werden – nämlich da, wo die Fehler beseitigt werden müssen. Aber auch eine technische Lösung kann den menschlichen Blick auf Ihre Systeme nicht ersetzen.

So sollten Sie bei der Planung des Monitoring vorgehen

Bevor ein Monitoring innerhalb einer Infrastruktur erfolgreich durchgeführt werden kann, müssen Sie ein Konzept erarbeiten. Dafür ist die Betrachtung der Informations- und Telekommunikations-Infrastruktur und der Anforderungen des Kernprozesses zwingend erforderlich. Wichtig ist, dass im ersten Schritt des Monitoring-Konzeptes eine Checkliste für alle notwendigen Technologien erstellt und natürlich dokumentiert wird.

Sie sollten bereits bei der Konzeption die zur Überwachung eingestuften Technologien in Ebenen unterteilen. Diese erleichtert die Wahl der Monitoring-Lösung erheblich und kann sogar Lizenzkosten sparen. Die definierten Ebenen sind kein Dogma und könnten je nach Anforderung beliebig erweitert werden.

Nachdem Sie alle wichtigen Technologien einmal manuell überwacht, die Ebene definiert und die Checkliste erstellt haben, lässt sich die Überwachung Schritt für Schritt automatisieren. Und auch beim Einsatz einer Monitoring-Lösung kann es sein, dass Sie stellenweise über Skripte beispielsweise Logdateien exportieren und gegebenenfalls sogar automatisch auswerten müssen. Oft macht Scripting mit XML, VBS oder Powershell diese Lösungen erst zu dem, was sie eigentlich sein sollen.

Monitoring-Lösungen und ihre Vor- und Nachteile

Bei der Wahl der Monitoring-Lösung kommt es immer darauf an, über welches Budget, welche personellen Ressourcen und natürlich welches Know-how Sie verfügen. Zur Erleichterung der Entscheidungsfindung werfen wir beispielhaft einen Blick auf Nagios, Brofmon/WinRM, Ipswitch WhatsUp Gold und Cacti. In den folgenden Abschnitten beschreiben wir die Vorzüge der einzelnen Lösungen auf der Basis der Ebenen.

Ebene 1: Physikalische Sicherheit

Nagios ist eine der flexibelsten Monitoring-Lösungen, die es überhaupt gibt. Da Nagios auf Open Source basiert, gibt es zahlreiche Erweiterungen in allen Bereichen. Gerade bei proprietärer Software scheitert es oft an fehlenden Plug-Ins

Nagios	Brofmon & WinRM	WhatsUp Gold	Cacti
Ebenen: Ebene 1, 2 und 3 Schranküberwachung Zutrittskontrolle Klimatisierung Geräteüberwachung Notstromversorgung Active Directory Virenschutz Datensiecherung Patchmanagement Firewallmanagement Webanwendung Portbelegung Verfügbarkeit Eventlogs SNMP	**Einsatzbereiche: Ebene 3** Active Directory Eventlogs Patchmanagement Webanwendung	**Einsatzbereiche: Ebene 2 und 3** Active Directory Eventlogs SNMP	**Einsatzbereiche: Ebene 2** Bandbreitennutzung Verfügbarkeit Übertragungsfehler Network-Access-Control SNMP
Vorteile: OpenSource keine Lizenzkosten Endlose Erweiterung Permanenter Scan Individuell anpassbar Basiert auf Schwellenwerten Alerting (SMS & Mail)	**Vorteile:** keine Lizenzkosten Endlose Erweiterung Individuell anpassbar Tabellarische Oberfläche Prüfungen via VBS möglich	**Vorteile:** Einfache Handhabung Alerting (Mail) Permanenter Scan	**Vorteile:** OpenSource keine Lizenzkosten Individuell anpassbar Grafische Visualisierung Permanenter Scan
Nachteile: Teilweise Agentbasiert Initiale Einrichtung sehr komplex	**Nachteile:** Nur zeitgesteuerte Aktualisierung Initiale Einrichtung sehr komplex	**Nachteile:** Lizenzkosten Erweiterung nicht grenzenlos möglich	**Nachteile:** Initiale Einrichtung sehr komplex

Bild 1: Beispielhafte Monitoring-Werkzeuge im Vergleich

für die SNMP-Abfragen von Schranküberwachung, Zutrittskontrolle, Klimatisierung oder Notstromversorgungen. Durch die große Nagios-Community kann diese Lösung über SNMP nahezu alle bereitgestellten Informationen auswerten.

Selbst die Darstellung sogenannter "Maps" ist ohne großen Aufwand möglich. Maps sind beispielsweise Topologien/Pläne von Netzwerkinfrastrukturen, Schrankbelegungen, Räumen oder sogar Standorten. Dabei kann anhand der Maps zur Schrankbelegung auch die Geräteüberwachung erfolgen oder sogar ein Dienststatus ausgegeben werden. Die Front-Ansicht der Serverschränke erleichtert dann auch das Auffinden des defekten Gerätes und kann selbst mit einem Raumplan gekoppelt werden. Dies ist natürlich auch standortübergreifend möglich, wobei hier verständlicherweise die Topologien etwas umfangreicher ausfallen.

Ebene 2: Netzwerk

Die Netzwerkebene dient der Überwachung von Bandbreitennutzung, Verfügbarkeit, Übertragungsfehlern und Network Access Control. Hier sollten Sie immer auf die Auswertung zeitbezogener Messdaten und ein schwellwertbasiertes Alerting setzen. Dabei lässt sich Nagios für das schwellenwertbasierte Alerting beim Verlust der Verfügbarkeit, Übertragungsfehlern oder bei der Nutzung des maximalen Traffics verwenden. Für das Sammeln oder Auswerten von Messdaten können Sie das RRD-Tool Cacti nutzen, das zum Beispiel ermöglicht, den Traffic zwischen zwei Netzwerkkomponenten zeitbasiert grafisch darzustellen. Bei Problemen können häufig Informationen wie Netzwerkauslastung oder -verfügbarkeit zu einer schnellen und unkomplizierten Lösung beitragen. Weiterhin ist es mit Cacti auch möglich, die Verläufe von Temperaturen oder auch Stromverbrauch aufzuzeichnen und darzustellen.

Ebene 3: Dienste

Für die kleine Windows-Infrastruktur mit wenigen Diensten und Servern ist die Kombination der Anwendungen Branche Office Monitor (kurz Brofmon) und Windows Remote Management (kurz WinRM) von Microsoft durchaus ausreichend. Leider setzen diese beiden Anwendungen viel Know-how in Sachen Visual Basic-Skript oder der Kommandozeile (Batch) voraus. In dieser Konstellation überwachen Sie mit Brofmon die Dienste, wobei lediglich Ausgabedateien der Kommandozeile auf Strings wie "error", "failed" oder "warning" geprüft werden. Innerhalb der Installation von Brofmon wird direkt die Auswertung des Befehls "dcdiag" konfiguriert. Zusätzlich sollten Sie gerade bei Domänencontrollern die Replikation, Zeitsynchronisation (NTP), DNS, DHCP und auch die

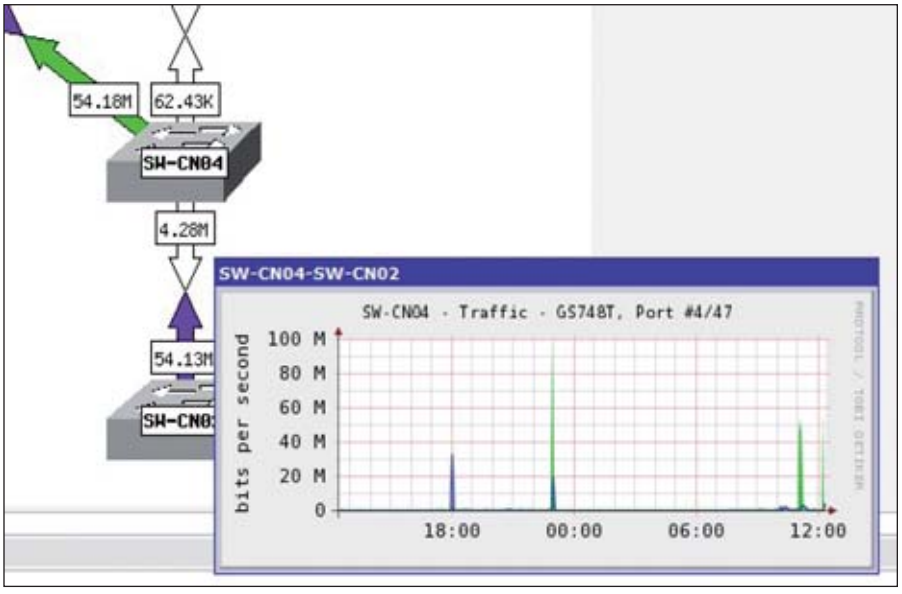


Bild 2: Die übersichtliche Anzeige des Switchstatus mit Cacti

Filereplikation überwachen. Diese Funktionen müssen jedoch manuell nachgepflegt werden. WinRM hingegen dient zur Sammlung der Ereignisprotokolle von Servern und ist seit Windows Vista/Server 2008 in jedem Microsoft-Betriebssystem enthalten.

Für die etwas größeren Infrastrukturen ist WhatsUp Gold von Ipswitch ein gutes Beispiel einer kommerziellen Lösung (die wir Ihnen in vergangenen Ausgaben des IT-Administrator bereits ausführlich vorgestellt haben). WhatsUp Gold ist zwar lizenzpflichtig, jedoch sehr einfach in der Grundinstallation und im Umgang. Sollten Sie jedoch über eine sehr individuelle IT-Infrastruktur verfügen, so ist Nagios die bessere und auch anpassbarere Monitoring-Lösung. Nagios kann beispielsweise ohne weiteres wichtige Dienste und Eigenschaften wie DHCP, DNS, Eventlog, LDAP oder RDP überwachen. Dazu zählt auch die Alarmierung bei der Vollauslastung der CPU oder des Festplatten-/Arbeitsspeichers. Zudem erlaubt Nagios auch Updates, die Aktualisierung der Virenpattern oder auch die erfolgreiche Erstellung von Backups zu überwachen.

Mögliche Stolpersteine beim Monitoring

Erfolgt das Monitoring noch von Hand, werden viele Probleme ausgeblendet, da die ausführende Person das Monitoring einfach über einen anderen Server oder die Anwendungen mit einem anderen Benutzerkonto öffnet. Dadurch werden Probleme wie fehlende Berechtigungen oder blockierte Netzwerkanfragen häufig erst bei der Implementierung der Monitoring-Lösungen aufgedeckt.

Manchmal kommt es sogar vor, dass das Monitoring netzwerkübergreifend geschehen soll, was jedoch nicht im Ansatz möglich ist, da die Netze gar nicht geroutet werden. Vorher war es kein Problem und ist nicht mal aufgefallen, da der Mitarbeiter immer an der Konsole des Servers gearbeitet hat. Zu guter Letzt kostet solch eine Monitoring-Lösung aus der Sicht der Lizenzen vielleicht nicht viel oder ist sogar kostenlos. Was auch passieren kann, ist, dass Lösungen vom Management häufig an der Ersparnis des Personals gemessen werden und der Mehrwert für das Unternehmen nicht berücksichtigt wird.

Fazit

Ein Monitoring ist für jede Umgebung erforderlich und wird dennoch viel zu oft vernachlässigt. Jeder verantwortungsbewusste IT-Leiter sollte sich zur Einführung eines Monitorings entschließen und die Implementierung sorgfältig planen. Auch bei den Monitoring-Lösungen gibt es gravierende Unterschiede, die Sie genau auf die Infrastruktur abstimmen sollten. *(jp)*

Sascha Giebelhausen ist Berater bei der adMERITia GmbH in Langenfeld.

Exchange Server 2010

Abgehängte Postfächer unmittelbar entfernen

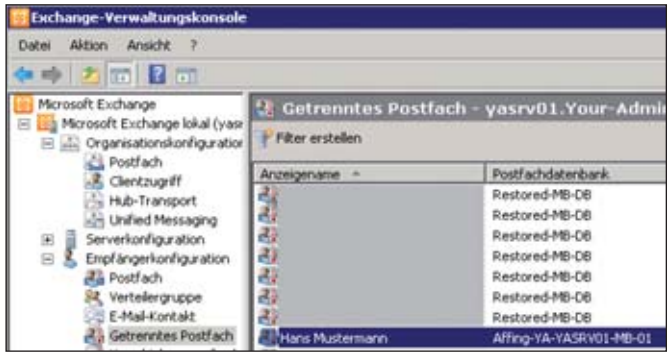
von Robert Lindermeier

Seit Exchange Server 2007 wurden sehr viele administrative Tasks in die Exchange Management-Shell verlagert. Viele Administratoren sehnen sich manchmal nach den "einfachen" Tasks, die in der Exchange Management-Konsole durchzuführen waren. So war es unter Exchange 2003 etwa noch möglich, über die Verwaltungskonsole ein soeben gelöschtes Postfach zu purgen, also sofort unwiderruflich zu entfernen. In der Exchange-Verwaltungskonsole finden Sie unterhalb der Empfängerkonfiguration einen Menüpunkt "Getrenntes Postfach". Dieser zeigt Ihnen alle Postfächer an, die von einem Benutzerkonto im AD getrennt sind. Hier besteht die Möglichkeit, ein abgehängtes Postfach wieder mit einem AD-Benutzerkonto zu verbinden. Per Default hält der Exchange Server ein abgehängtes Postfach 30 Tage zur Wiederherstellung vor.

Allerdings fehlt hier der von Exchange 2003 gewohnte Menüpunkt "Postfach leeren (entfernen)". Diese Funktion ist nur noch über die Exchange Management-Shell ausführbar. Insbesondere, wenn das Postfach erst kurz zuvor entfernt wurde, dauert es ohne weitere Befehle geraume Zeit, bis das Postfach unter "Getrenntes Postfach" sichtbar wird. Genau dieser Vorgang lässt sich jedoch beschleunigen. Mit dem Kommando

```
Get-MailboxDatabase | Clean-Mailbox-
  Database
```

weisen Sie den Exchange Server an, in allen Postfachdatenbanken nach gelöschten Postfächern zu suchen, indem eine Synchronisation mit dem Active Directory durchgeführt wird. Nun wird ein zuvor gelöschtes Postfach sichtbar, wie in unserem Bild-Beispiel "Hans Mustermann". Sie können sich nun auch die entsprechenden Postfächer in der Exchange Management-Shell mit folgendem Kommando anzeigen lassen und erkennen an "DisconnectDate", dass es sich um eine entfernte Mailbox handelt:



Die Suche nach gelöschten Postfächern macht diese in der Admin-Konsole sichtbar

```
Get-MailboxStatistics -Database
  "{Name-Datenbank}" | FL Display-
  Name, DisconnectDate, MailboxGuid
```

Um nun eine abgehängte beziehungsweise gelöschte Mailbox endgültig aus dem Postfachspeicher zu entfernen, benötigen Sie die MailboxGuid im nächsten Kommando. Kopieren Sie diese aus dem angezeigten Ergebnis und bauen Sie die Guid in den nachfolgenden Befehl ein, um die Mailbox endgültig zu entfernen:

```
Remove-Mailbox -Database "{Name der
  Datenbank}" -StoreMailboxIdentity
  "3a10fce8-4c3a-4b8a-8ccf-
  df4d38a86f04"
```

Nun erhalten Sie die Sicherheitsabfrage "Möchten Sie diese Aktion wirklich ausführen?", die Sie mit "J" bestätigen. Sollten Sie auf eine solche Bestätigungsabfrage verzichten können, dann fügen Sie als weitere Option "Confirm:$False" zum Befehl *Remove-Mailbox* mit an. Das Postfach wird dann ohne weitere Rückfrage entfernt. Um nun mehrere abgehängte Postfächer in einer Datenbank mit einem Befehl zu entfernen, zeigt sich einer der vielen Vorteile der Exchange Management-Shell. Ein einfaches Filterkommando ermöglicht es, auf einen Schlag alle abgehängten Postfächer zu entfernen. Sehen Sie sich das im Detail mal an: Über *Get-MailStatistics* holen Sie eine Liste aller Postfächer und schicken diese über die Pipe (|) durch den Filter. *Where* .... prüft nun, ob beim aktuell bearbeiteten Postfach ein Wert im Feld "DisconnectDate" steht. Das Ergebnis fließt dabei als Eingabe in den Remove-Mailbox-Befehl und über die MailboxGuid werden die abgehängten Postfächer entfernt:

```
Get-MailboxStatistics | Where {
  $_.DisconnectDate -ne $null } |
  Remove-Mailbox -Database "{Name-
  Datenbank}"  -StoreMailboxIdentity
  $_.MailboxGuid -Confirm:$false
```

Damit haben Sie alle Postfächer, die einen Wert im Feld "DisconnectDate" tragen, ohne weitere Bestätigung entfernt. *(dr)*

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

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.

Microsoft Windows

Ich bin ein **begeisterter Nutzer der PowerShell**. Die Kommandozeile existiert in Version 2.0 ja auch in einer Variante für Windows XP, Server 2003 und Vista – einige Bestandteile wie etwa das Active Directory-Modul stehen jedoch nur unter Windows 7 oder Server 2008 R2 zur Verfügung. Nun habe ich gehört, dass sich die eigentlich nur für die neuen OS-Versionen gedachten **PowerShell-Module an älteren Rechner remote ausführen** lassen. Können Sie beschreiben, wie das genau geht und wie hierfür die Voraussetzungen sind?

Um PowerShell-Module, die eigentlich nur für Windows 7 und Server 2008 R2 gedacht sind, remote auch auf anderen Windows-Versionen bereitzustellen, benötigen Sie logischerweise mindestens einen Computer im Netzwerk, der unter einem der aktuellsten Betriebssysteme läuft. Wenn Sie das Active Directory-Modul verwenden wollen, bietet sich die Installation eines Domänencontrollers unter Server 2008 R2 an, da auf diesem sowohl das Modul selbst als auch der Active Directory Management Gateway Service (Link-Code: B2PE3) läuft, der beim Einsatz des Moduls nötig ist.

Geben Sie als Erstes in der PowerShell des neuen Domänencontrollers das Kommando *Enable-PSRemoting* ein – nur dann funktioniert der Remote-Zugriff auf den Server. Alle weiteren Schritte führen Sie nun von einem XP- oder Server 2003-Rechner aus. Starten sie dort die Powershell und stellen Sie mit dem Kommando

```
$session = New-PSSession -computer-
  Name <Neuer Domänencontroller>
```

eine Verbindung zum Remote-Rechner her. Danach starten Sie auf dem entfernten Rechner mit folgendem Befehl die Active Directory-CMDlets:

```
Invoke-command {import-module acti-
  vedirectory} -session $session
```

Nun müssen Sie noch dafür sorgen, dass das Modul auf Ihren Computer wandert. Dies geschieht mit dem Kommando

```
Export-PSSession -session $session
  -commandname *-AD* -outputmodule
  RemAD -allowclobber
```

Der Parameter "*-AD*" sorgt hier dafür, dass nur CMDlets mit dem entsprechenden Prefix, in diesem Fall also Active Directory-relevante, geladen werden. Der Befehl legt die CMDlets jedoch nicht direkt auf dem XP-Rechner ab, sondern erstellt im Ordner "WindowsPowerShell \ Modules \ RemAD" lediglich eine Verknüpfung, die auf die Remote-Verbindung verweist. Nun können Sie mit dem eigentlich nicht unter XP lauffähigen Modul arbeiten. Beenden Sie dazu allerdings zunächst mit dem Befehl

```
Remove-PSSession -session $session
```

die bestehende Remote-Sitzung – das CMDlet starten Sie remote allein durch folgende Eingabe:

```
Import-Module RemAD -prefix Rem
```

Das Modul wird nun in den Speicher geladen – erweitert um das Prefix "Rem", das Sie bei der Arbeit mit dem Modul stets eingeben müssen und das Sie an den Remote-Charakter des CMDlets erinnert. Nun stehen Ihnen alle Befehle des Moduls zur Verfügung. Mit dem Kommando

```
Get-RemADUser -filter "Name
  -like 'D*'"
```

etwa lassen Sie sich alle AD-Nutzer ausgeben, die mit "D" beginnen. Der Befehl sucht die entsprechenden Objekte auf dem Remote-Rechner heraus, überführt Sie in das XML-Format, sendet diese Liste an den XP-Rechner und setzt sie dort wieder in AD-Objekte um, die Sie mittels Pipelining in weiteren Kommandos verwenden können. Die durch den Befehl geöffnete Remote-Session bleibt so lange geöffnet, bis Sie die PowerShell schließen oder aber mit der Eingabe von

```
Remove-Module RemAD
```

das Modul wieder aus dem lokalen Speicher entfernen. *(ln)*

Bei einem Admin-Treffen hat mir ein Kollege erzählt, dass er es **mittels einer CSV-Datei und einer kurzen Befehlszeile** in der PowerShell geschafft hat, sehr schnell eine **große Anzahl von neuen Active Directory-Benutzern anzulegen**. Leider reichte die Zeit bei dem Admin-Treffen nicht mehr aus, um mir die genaue Vorgehensweise zu erklären. Können Sie hier einspringen?

Ihr Kollege hat recht. Mittels einer CSV-Datei und zwei per Pipe verbundenen CMDlets lässt sich erledigen, was sonst nur ein mehrzeiliges VBScript bewirken könnte – nämlich das Anlegen einer Vielzahl neuer AD-User mit ein paar Tastenklicks. Zunächst einmal benötigen Sie eine CSV-Datei mit den Daten der neuen User. Wichtig dabei ist, dass die Spaltenüberschriften genau mit den Parameternamen des New-ADUser-CMDlets übereinstimmen. Eine per Komma getrennte CSV-Datei könnte also folgendermaßen aussehen:

```
Surname,GivenName,Department,Name
Clever,Fred,Spionage,FredC
Simpson,Homer,Sicherheit,HomerS
Duck,Dagobert,Finanzen,DagobertD
```

Geben Sie nun in der Powershell folgendes Kommando ein, um aus dem Datensatz neue Benutzer anzulegen:

```
Import-CSV c:\new-users.csv
  | New-ADUser
```

Das CMDlet *Import-CSV* gibt für jede Zeile in der CSV-Datei ein Objekt aus. Diese Objekte verfügen über Eigenschaften, die den CSV-Spaltenüberschriften entsprechen. Da die CSV-Datei sämtliche erforderlichen Parameter für *New-ADUser* enthält, müssen Sie keine weiteren Parameter mehr manuell angeben. Zusätzliche, nicht in der Datei hinterlegte Parameter sind möglich und für jeden neu erzeugten Benutzer gültig. Mit

```
Import-CSV c:\new-users.csv
  | New-ADUser -organization
  "{Firmenname}"
```

etwa können Sie einen allgemeingültigen Firmennamen setzen. Die neuen Benutzer sind angelegt – wichtig ist für diesen Schritt wie bereits erwähnt, dass die Spaltenüberschriften exakt den CMDlet-Parameternamen entsprechen. *(ln)*

Auf einem nicht im Unternehmensnetzwerk hängenden Test-Notebook probiere ich Tools zunächst immer aus, bevor ich sie im praktischen Betrieb verwende. Was ich etwas hinderlich finde, ist die Tatsache, dass **Windows 7 beim Starten des Systems stets ein Benutzerkennwort verlangt**, selbst wenn es nur einen User gibt. Unter XP ließ sich das Betriebssystem ja noch **ohne Kennwort starten**. Ist dies irgendwie auch unter Windows 7 möglich? In der Systemeinstellung habe ich dazu nichts gefunden.

Seit Windows Vista verlangt Microsoft, dass sich der Benutzer mit einem Passwort am System anmeldet. Diese obligatorische Eingabe lässt sich aber deaktivieren – zwar nicht über die Systemsteuerung, aber über ein Kommando in der Eingabeaufforderung. Verwenden Sie dazu den Befehl *control userpasswords2*. Beachten Sie, dass Sie dieses Kommando nur ausführen können, wenn Sie als Administrator angemeldet sind. Nun erscheint ein Fenster, das sämtliche auf dem Rechner vorhandenen Benutzerkonten anzeigt. Wählen Sie das entsprechende Konto aus und entfernen Sie den Haken bei "Benutzer müssen Benutzernamen und Kennwort eingeben". Nach einem Klick auf "OK" müssen Sie zur Sicherheit noch einmal das Kennwort des jeweiligen Benutzers eintippen. Beim nächsten Neustart funktioniert die Anmeldung auch ohne Passwort. *(ln)*

Linux

Auf einigen Notebooks in unserem Unternehmen läuft als Betriebssystem openSUSE 11.2. Hier gibt es ja ein **Verzeichnis, in dem das OS alle temporären Dateien sammelt**. Um Datenmüll zu vermeiden, würde ich diesen Ordner gerne öfter **regelmäßig leeren**. Gibt es irgendeinen Weg, die entsprechenden Einstellungen im System über eine grafische Oberfläche zu verändern, ohne dass ich mich mit dem Text-Editor durch die Konfigurationsdateien schlagen muss?

Das in openSUSE ab Version 10.1 integrierte Konfigurationswerkzeug YaST (Yet another Setup Tool) erspart Ihnen in dem von Ihnen beschriebenen Fall die Arbeit mit einem Texteditor. Starten Sie den Sysconfig-Editor über das Yast-Modul "System / Editor für /etc/sysconfig-Dateien". Im nun erscheinenden Fenster entspricht die Baumstruktur links den aus dem Verzeichnis "/etc/sysconfig" bekannten Konfigurationsdateien. Klicken Sie auf die Schaltfläche "Suche" und aktivieren Sie nun die Optionen "Variablennamen suchen" und "Beschreibung suchen". Als Suchbegriff geben Sie dann "tmp" ein. Nun erscheint im linken Bereich des Fensters eine logische Aufstellung von Systemeinstellungen, die zu Ihrem Suchbegriff passen. Weit oben in der Liste müsste der Parameter "MAX_DAYS_IN_TMP" zu finden sein. Wählen Sie diesen Eintrag aus und verändern Sie oben rechts in der Eingabezeile den Standardwert "0" etwa auf "7". In diesem Fall entfernt die Jobsteuerung cron beim nächsten Durchlauf alle TMP-Dateien, auf die länger als sieben Tage nicht zugegriffen wurde. Wollen Sie gewisse Dateien von dieser automatischen Löschung ausnehmen, so hinterlegen Sie diese bei der Einstellung "OWNER_TO_KEEP_IN_TMP". Vergessen Sie nicht, die neuen Settings durch einen Klick auf die Schaltfläche "Beenden" zu speichern. *(ln)*

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

Ich benutze **KVM und XEN als Hypervisor** für meine virtuellen Maschinen. Als Backend für die Maschinen verwende ich ausschließlich Image-Dateien im lokalen Dateisystem. Eine meiner virtuellen Maschinen bootet jedoch nicht mehr, ich vermute einen **Tippfehler in der Bootloader-Konfigurationsdatei**, die ich kürzlich manuell editiert habe. Wie kann ich das Problem lösen?

Image-Dateien lassen sich ohne weiteres mit dem Tool kpartx in einzelne Partitionen zerlegen:

```
# kpartx -l
  /var/lib/libvirt/images/rhel6.img
loop0p1 : 0 1024000 /dev/loop0 2048
loop0p2 : 0 11556864 /dev/loop0
  1026048

# kpartx -a
  /var/lib/libvirt/images/rhel6.img
add map loop0p1 (253:2): 0 1024000
  linear /dev/loop0 2048
add map loop0p2 (253:3): 0 11556864
  linear /dev/loop0 1026048
```

Die so erzeugten Loop-Geräte liegen anschließend im Verzeichnis "/dev/mapper" und lassen sich ganz regulär in das Dateisystem einbinden:

```
# ll /dev/mapper/loop*
lrwxrwxrwx. 1 root root 7 Jan 11
  20:13 /dev/mapper/loop0p1 ->
  ../dm-2
lrwxrwxrwx. 1 root root 7 Jan 11
  20:13 /dev/mapper/loop0p2 ->
  ../dm-3

# mount /dev/mapper/loop0p1
  /mnt/rhel6-disk1

# df -h /mnt/rhel6-disk1
Filesystem Size Used Avail Use%
  Mounted on
/dev/mapper/loop0p1 485M 54M 406M
  12% /mnt/rhel6-disk1
```

Sind alle Änderungen durchgeführt, können Sie die Verknüpfungen der Loop-Geräte mit den Partitionen der Image-Datei wieder lösen:

```
# kpartx -d
  /var/lib/libvirt/images/rhel6.img
loop deleted : /dev/loop0
```

(Thorsten Scherf/ln)

Ich bin noch nicht so firm, was die Bedienung der **Exchange-Verwaltungsshell** angeht. Gerade was die Verbindung von Benutzerkonten im Active Directory mit Postfächern in Exchange betrifft, erscheint mir der Weg über die Shell aber sehr sinnvoll. Welche CMDlets würden Sie empfehlen, wenn es darum geht, die **Berechtigungen eines AD-Benutzerkontos für ein bestimmtes Postfach herauszufinden?**

Wenn Sie lediglich wissen möchten, über welche Berechtigungen ein AD-Benutzerkonto für ein spezifisches Postfach verfügt, dann verwenden Sie den folgenden Befehl:

```
Get-Mailbox {Zu überprüfende Mail-
  box} | Get-MailboxPermission
  -User {AD-Benutzer}
```

Wenn Sie hingegen herausfinden wollen, für welche Postfächer ein bestimmter Active Directory-Benutzer überhaupt Berechtigungen besitzt, dann geben Sie folgendes Kommando ein:

```
Get-Mailbox -ResultSize Unlimited |
  Get-MailboxPermission -User {AD-
  Benutzer} | Format-Table Identity,
  AccessRights, Deny
```

Bei der Anwendung dieses Befehls sollten Sie sich aber darüber im Klaren sein, dass er alle Postfächer in Ihrer Organisation auflistet. Wenn Sie über eine große Anzahl von Postfächern verfügen, sollten Sie sich also auf bestimmte Postfächer beschränken. *(ln)*

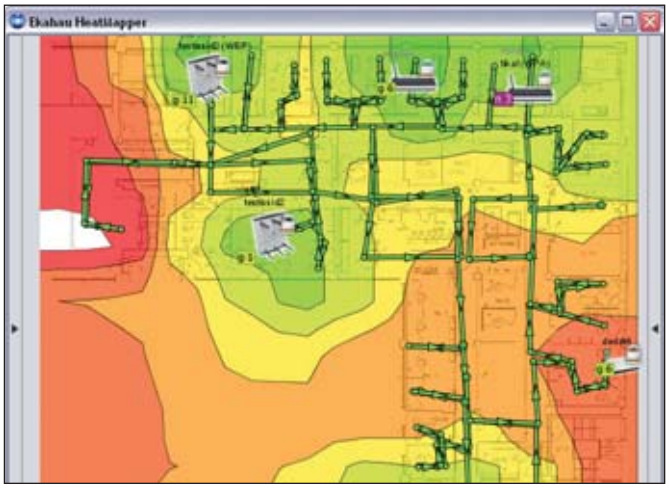
Tools

Wer eine **komplexe Active Directory-Domänenstruktur** mit großen Fileservern betreibt, auf die viele Benutzer mit unterschiedlichen Rechten zugreifen, weiß, wie schwer es ist, allein mit den Windows-Bordmitteln auf Dauer einen genauen Überblick über die Zugriffsrechte zu behalten. Vor allem fällt es schwer, schnell die effektiven Rechte zu erkennen und Verschachtelungen zu vermeiden. Um nicht irgendwann im selbstgeschaffenen Dschungel zu enden, gehen viele Administratoren beispielsweise dazu über, die Rechte im Dateisystem nur auf den ersten beiden Verzeichnisebenen zu vergeben, so dass weiter unten nur die normale Vererbung greift. Über eigene Regeln wie diese steht dann fest, wie weit die Verzeichnisstruktur durchforstet werden muss, wenn es darum geht, Berechtigungen nachzuvollziehen. Verschärft wird die Situation in vielen Unternehmen durch regelmäßige organisatorische Umstrukturierungen, die es erforderlich machen, die Verzeichnisstrukturen und die damit verknüpften Rechte anzupassen, wobei dann die Gefahr besteht, dass die Berechtigungen im Laufe der Zeit stark aufweichen.

Das kostenlose Werkzeug **Permissions Analyzer for Active Directory** von Solarwinds erlaubt über ein Dashboard auf dem Desktop eine **komplette hierarchische Ansicht aller effektiven Berechtigungen und Zugriffsrechte** eines Dateiordners oder eines Shares. Gleichzeitig gewährt das Tool Einblicke in die Rechte einzelner User und den Ursprung dieser Rechte (Gruppenmitgliedschaften und direkte Berrchtigungen). So kann der Administrator komfortabel durch die Rechtestruktur seines Active Directory browsen und User-Rechte detailliert analysieren. Das Tool steht nach einer Registrierung zum freien Download zur Verfügung. *(jp)*

Link-Code: B2PE1

Setzt ein Unternehmen komplett oder teilweise auf eine WLAN-basierte Vernetzung der Arbeitsplätze, gibt es viele



Die mit dem HeatMapper erstellte Landkarte zeigt anschaulich, wo das WLAN Löcher in der Signalstärke aufweist

gute Gründe sicherzustellen, dass die **Access Points optimal im Gebäude verteilt** sind. So lassen sich Funklöcher vermeiden oder auch Überlappungen der Funkzellen ausschließen, was die Anzahl der benötigten APs reduziert.

Die freie Software **Ekahau HeatMapper** ermöglicht die Erstellung einer Landkarte der eigenen WLAN-Infrastruktur. Mit dem Tool und einem Laptop ausgestattet kann der IT-Verantwortliche so die **Struktur und die Abdeckung des WLANs ermitteln**. Das Tool erlaubt dabei, entweder eine komplette Karte der Struktur zu erstellen oder die Analyse der Reichweite einzelner APs vorzunehmen. Dazu lädt der Admin zunächst einen selbst erstellten oder eingescannten Grundriss des Gebäudes ein (oder startet mit einer leeren Karte). Das Tool findet nun verfügbare WLAN-Router beziehungsweise APs selbstständig. Der Anwender geht mit dem Notebook langsam durch das Gebäude und markiert die gewünschten Mess-Standorte jeweils auf der virtuellen Gebäudekarte. Mit diesen Daten erstellt Ekahau HeatMapper sehr übersichtlich, wie es um die Empfangsstärken in den verschiedenen Räumlichkeiten der Gebäude bestellt ist. Sind mehrere WLAN-Sender vorhanden, wechselt die Darstellung für jedes Gerät beim Überfahren mit der Maus, ideal bei Verwendung von mehreren WLAN-Stationen. Darüber hinaus zeigt der HeatMapper Sicherheitsprobleme auf, indem er den Anwender beispielsweise auf ungesicherte Zugangspunkte hinweist. Gleichzeitig lässt sich die komplette Konfiguration der APs einsehen. Auch hier ist für den kostenlosen Download eine kurze Registrierung erforderlich. *(jp)*

Link-Code: B2PE2

Tauchen auf **ESX- oder ESXi-Servern Probleme** auf, so kann das **Troubleshooting** eine ziemliche Herausforderung sein. Administratoren auf Problemsuche können da jede Hilfe gut gebrauchen. Vor allem benötigen sie ein verlässliches Management-Tool, das den IT-Verantwortlichen genau zeigt, was in den virtuellen Maschinen vor sich geht.

Das kostenlose Werkzeug **Xangati for ESX** bietet als **virtuelle Appliance** eine genaue Sicht auf die Kommunikationsaktivität jeder einzelnen VM innerhalb eines VMware ESX-Hosts. Das Tool liefert dem Administrator dabei **Antwort auf die Fragen nach dem Verhalten einer bestimmten VM**, mit wem eine VM kommuniziert und welche Anwendungen dort ausgeführt werden. Zudem teilt Xangati dem Admin mit, welche Endbenutzer aktuell auf eine VM zugreifen und wie viel Bandbreite jeder Benutzer, jede Anwendung, jedes Protokoll und jeder Port verbraucht. Xangati for ESX in der freien Version (beschränkt auf die Überwachung eines ESX-Hosts, ansonsten aber sind alle Features enthalten, die die kostenpflichtigen Versionen bieten) ist speziell für den Einsatz in kleineren ESX-Installationen konzipiert. Im Detail leistet die kostenlose Version Folgendes für den Administrator:

- Auto-Discovery und -Naming der VMs und Applikationen im ESX-Host
- Echtzeit-Darstellung von mehr als 100 Parametern des Hosts und der Gäste (inklusive CPU, Speicher, Festplatten und Latenz des Storage)
- Einsicht in die vSwitch-Kommunikation
- 12-wöchige Historie der Reports

Für den Download der freien Version von Xangati ist lediglich eine kurze Registrierung auf der Seite des Herstellers erforderlich. Im Anschluss daran erhält der Interessent den Link zum Download per E-Mail. *(jp)*

Link-Code Download: B1PE4

Link-Code Installationsanleitung: B1PE5

Xangati for ESX stellt mehr als 100 Parameter der virtualisierten Infrastruktur in Echtzeit dar

Mit Fraud-Management-Werkzeugen Insiderdelikte verhindern und aufdecken

Der Feind in meinem Haus

von Stephan Sippel

Quelle: Cory Thoman – Fotolia.com

Insiderdelikte bedrohen heute Unternehmen jeder Größenordnung und haben nicht nur direkte finanzielle Schäden zur Folge, sondern zerstören auch das Vertrauen der Kunden und können irreparable Imageschäden hinterlassen. In seinem Bericht 2010 stellt der US-Verband Association of Certified Fraud Examiners fest, dass Unternehmen pro Jahr im Mittel fünf Prozent ihrer jährlichen Umsatzerlöse aufgrund von Betrugsdelikten verlieren. Weltweit summiert sich dies auf eine Summe von fast 2,9 Billionen US-Dollar. Erschreckend ist, dass die meisten Menschen, die sich unbefugt Zugang zu IT-Systemen und Daten verschaffen, diejenigen sind, die in einer Organisation das größte Vertrauen genießen: Mitarbeiter, Auftragnehmer und Geschäftspartner. Ihr Insiderwissen über Geschäftsprozesse und Sicherheitskontrollen in Verbindung mit ihrem legalen Zugang zu wichtigen Systemen versetzt sie in die besondere Lage, Daten zu manipulieren und wertvolle Ressourcen zu stehlen. Wie Sie Insiderdelikte aufklären und vermeiden, zeigt dieser Beitrag.

Mit herkömmlichen Verfahren zur Erkennung von Betrugsdelikten wie der Protokollierung von Anwendungen sind Unternehmen nicht in der Lage, mit dem Umfang und der Komplexität heutiger Bedrohungen fertig zu werden. Doch moderne Technologien eröffnen neue Möglichkeiten, diesem Problem Herr zu werden. Sogenannte Enterprise-Fraud-Management-Lösungen ermöglichen die unternehmensweite Erkennung und Vermeidung von Betrugsdelikten, um Benutzeraktivitäten unter allen Anwendungen zu erfassen und zu analysieren. Sie führen zudem eine genaue und belegbare Überwachung der Anwendungen durch und erstellen daraus aussagekräftige Informationen als Grundlage für fundierte Entscheidungen.

Warum Insiderdelikte schwer zu erkennen sind

Firewalls, Virtual Private Networks (VPNs) und Intrusion Detection Systems (IDSs) leisten wirksame Dienste, um den unbefugten Zugriff externer Personen auf Informationen und Ressourcen zu unterbinden. Doch diese Sicherheitskontrollen sind gegen böswillige Insider wirkungslos, die aufgrund ihrer Vertrauensstellung das Recht haben, auf Anwendungen zuzugreifen, Datenbanken abzufragen und Systemkonfigurationen zu ändern. Böswillige Insider können für sich drei Faktoren ausnutzen:

1. Zugriff auf mehrere Anwendungen: Mitarbeiter mit Zugriff auf mehrere Anwendungen können hintereinander mehrere Aufgaben durchführen, die einen legitimen Eindruck erwecken. Beispielsweise könnte ein Mitarbeiter, der berechtigt ist, einen offenen Posten für einen Lieferanten anzulegen, auch einen fingierten Lieferanten im System anlegen und Zahlungen an dieses Unternehmen tätigen. Eine mögliche Lösung – nämlich die Aufgabentrennung – ist nicht immer machbar. Ein Manager benötigt zum Beispiel Zugriff auf mehrere Anwendungen, um Fehler zu berichtigen, bestimmte Transaktionen zu genehmigen oder nicht administrative Vorgänge durchzuführen.
2. Kenntnis der Geschäftsprozesse: Mitarbeiter, die jahrelang in derselben Ab-

teilung tätig sind, sind mit Arbeitsabläufen und Vorgängen bestens vertraut; auch mit der Behandlung von Ausnahmen und Überwachungsprozeduren. Ein Mitarbeiter im Rechnungswesen, der beispielsweise geschäftliche Berichte erstellt und Daten an die Wirtschaftsprüfer weitergibt, weiß, welche Transaktionen wahrscheinlich geprüft und welche nicht geprüft werden.

3. Unterlaufen protokollbasierter Überwachungskontrollen: Mitarbeiter mit detaillierten Kenntnissen der Protokollverfahren können diese Verfahren unterlaufen, um unentdeckt zu bleiben. Werden Eingriffe von Managern, die die regulären Verfahren außer Kraft setzen, beispielsweise stets protokolliert und geprüft, kann der betreffende Mitarbeiter diese Vorgehensweise vermeiden und stattdessen falsche Transaktionen erzeugen, die er unter die routinemäßigen Transaktionen mischt.

Diese drei Faktoren machen es schwer, Insiderdelikte mit herkömmlichen Verfahren zu bekämpfen. Eine wirksame Risikomanagementstrategie muss diese Schwachstellen unbedingt berücksichtigen.

Wo Protokollierung nicht weiterhilft

Die Anwendungsprotokollierung wurde als wichtiges Werkzeug für das Management von IT-Operationen und -Systemen entwickelt. Sie diente also ursprünglich nicht zu Prüfungszwecken und zur Betrugsbekämpfung. Anwendungsprotokollierung wurde erst deshalb zum Standardverfahren, weil es bisher keine echte Technologie zur Anwendungsüberwachung gab. Mit zunehmender Verbreitung und wachsender Funktionalität von Enterprise-Anwendungen wird die Fähigkeit, die herkömmliche Protokollierung als moderne Lösung gegen Betrugsdelikte einzusetzen, aus zwei Gründen unhaltbar.

Isolierte Protokolleinträge

Betrugsdelikte setzen sich ebenso wie Geschäftsprozesse aus mehreren Schritten zusammen und umfassen üblicherweise mehrere Anwendungen. Jeder Schritt kann Teil eines wichtigen Geschäftsprozesses und Teil eines Betrugsversuchs sein: Eine in eine Webanwendung eingegebene Transaktion, eine Änderung an einer Abteilungsdatenbank durch eine andere Abteilung und eine Abfrage über ein Mainframesystem.

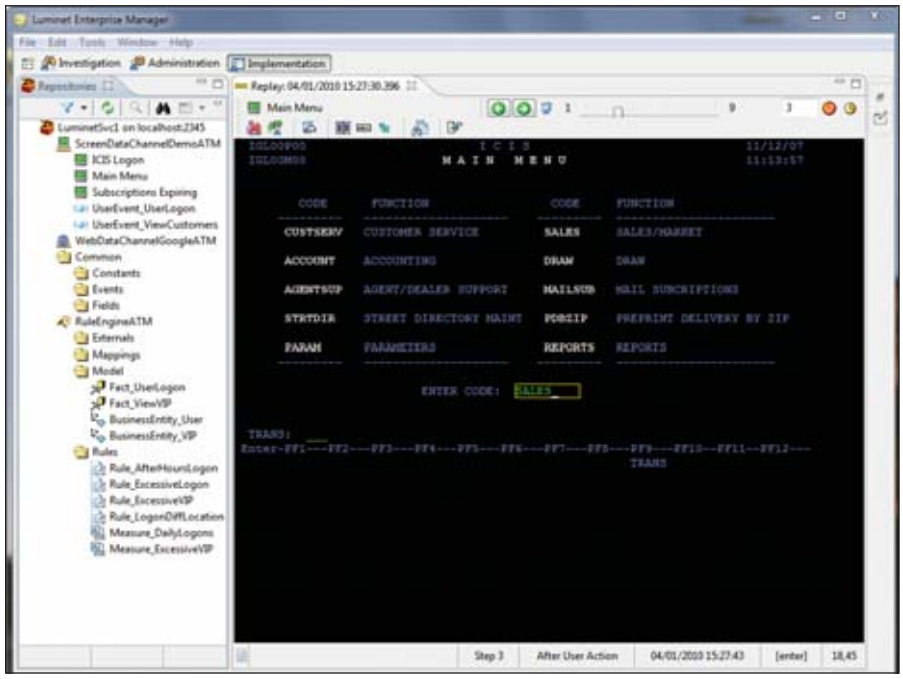


Bild 1: Die visuelle Wiedergabefunktion der Fraud-Management-Software "Attachmate Luminet" ermöglicht eine stille Beobachtung der Benutzeraktivitäten auf Ebene jedes Fensters und jeder Tasteneingabe

Andererseits konzentriert sich die herkömmliche Protokollierung üblicherweise auf eine einzelne Anwendungskomponente, etwa eine Datenbank, einen Anwendungsserver oder ein Messaging-Subsystem. Jede Komponente erzeugt ein anderes Protokoll mit unterschiedlicher Informationsfülle in unterschiedlichen Formaten. Isolierte Protokolleinträge zu einzelnen Ereignissen in einer Komponente sind nur schwer mit den in anderen Protokollen aufgezeichneten Ereignissen in Beziehung zu setzen. Schon ein Server, dessen Systemzeit nicht synchronisiert ist, kann die Zusammenführung von Daten aus zwei Protokolldateien erschweren. Protokolle arbeiten zudem mit unterschiedlichen Datentypen und Formaten. Wer diese Informationen interpretieren will, muss das Glück auf seiner Seite haben und viel Sachverstand mitbringen.

Unvollständige Daten

Wer die Anwendungsprotokolle für die Erkennung von Insiderdelikten heranziehen möchte, wird schon aufgrund der unvollständigen Informationslage auf Schwierigkeiten stoßen. Nur ein Bruchteil des Dialogs zwischen Mitarbeitern und Anwendungen wird von den herkömmlichen Protokollen erfasst. Das bedeutet im Umkehrschluss: Eine lückenlose Beweisführung ist gar nicht möglich. Doch ohne vollständige und belastbare Informationen sind keine fundierten Maßnahmen möglich.

Ein Beispiel: Eine Datenbank protokolliert die Aktualisierung eines Kontos, wobei der ursprüngliche und der neue Saldo aufgezeichnet werden. Diese Informationen sind zwar für die IT-Systemverwaltung nützlich, aber für kriminalistische Nachforschungen fehlen wichtige Angaben:

- Die Identität des Benutzers, der die Aktualisierung durchgeführt hat.
- Das zur Aktualisierung verwendete Anwendungsmodul.
- Verknüpfungen zu Ereignissen, die vor und nach der Aktualisierung stattgefunden haben.

Auch wenn Anwendungsentwickler diese Informationen berücksichtigen wollten, stünden sie auf Datenbankebene möglicherweise gar nicht zur Verfügung. Aus Leistungsgründen werden Datenbankverbindungen üblicherweise über ein einziges Datenbankbenutzerkonto gebündelt. Die Identität des Anwendungsbenutzers ist daher auf den unteren Ebenen der Datenbanktransaktion gar nicht einsehbar. Angesichts der begrenzten Fähigkeit, eine Untermenge aller potenziell nützlichen Informationen nachzuvollziehen und aufzuzeichnen, eignet sich die Protokollierung für die Anforderungen einer unternehmensweiten Überwachung und Beobachtung nicht. Aufgrund der Einschränkungen herkömmlicher Protokollierungsverfahren ist eine grundsätzlich andere Herangehensweise erforderlich.

Sichere Multichannel-Überwachung

Softwarelösungen zur Bekämpfung von Insiderdelikten heben die mit der Protokollierung einzelner Anwendungskomponenten verbundenen Einschränkungen auf. Sie erfassen eine vollständige Historie der Benutzeraktivitäten im Netzwerk, um ohne kostspielige Modifikationen an vorhandenen Anwendungen eindeutige und rechtskräftige forensische Nachweise zusammenstellen zu können.

Solche Werkzeuge sammeln alle Benutzeraktivitäten wie ein stiller Beobachter. Insidern ist es daher nicht möglich, einer Entdeckung zu entgehen, indem sie ihre Aktivitäten über mehrere Anwendungen aufteilen. Ein Benutzer könnte beispielsweise in der Lage sein, die Auslösung von Warnmeldungen in einer einzelnen Anwendung zu vermeiden oder Änderungen an einer Datenbank unter Umgehung der Bedienoberfläche vorzunehmen, um so der Protokollierung des Ereignisses zu entgehen. Diese Maßnahmen würden einer herkömmlichen Überwachung durch Protokollierung möglicherweise entkommen, hinterließen aber dennoch Spuren im Netzverkehr.

Bild 2: Moderne Analysewerkzeuge machen Aktivitätsmuster und komplexe Beziehungen im Unternehmen transparent

Ein weiterer Vorteil ist die Abdeckungsbreite. Die Interaktion zwischen Benutzern und Anwendungen kann über komplexe Arbeitsabläufe, Middleware, Messaging-Dienste oder den direkten Datenbankzugriff erfolgen. Diese Aktivitäten werden aufgezeichnet und in einem sicheren Repository gespeichert. Dort stehen sie für Suche, Abruf und Wiedergabe beliebiger Teile der vollständigen Historie eines Benutzers jederzeit zur Verfügung. Daher lassen sich zudem detaillierte und aggregierte Berichte, Warnmeldungen und Dashboards erstellen, um verdächtige Aktivitäten aufzuspüren, einzuordnen und zu untersuchen: Greift ein Manager deutlich öfter auf vertrauliche Kundeninformationen zu als andere? Fällt ein Mitarbeiter aus dem Rechnungswesen durch ungewöhnliche Zahlungsaktivitäten in Bezug auf einen bestimmten Lieferanten auf?

Nach Extraktion dieser Informationen ist eine unverzügliche Untersuchung möglich, ohne darauf warten zu müssen, dass die IT-Abteilung kryptische Log-Dateien abruft und in stundenlanger Arbeit manuell auswertet. Mit Fraud-Management-Lösungen ist es möglich, einen Drilldown von der automatischen Warnmeldung zu den Risikobewertungsberichten durchzuführen und auf Anhieb genau die Aktionen zu untersuchen und wiederzugeben, die die verdächtigen Benutzer durchgeführt haben – Schritt für Schritt und Bildschirm für Bildschirm. So setzt sich das Puzzle zu einem aussagekräftigen Bild zusammen.

Fazit

Die meisten Unternehmen sehen sich vor immer strengere gesetzliche und aufsichtsrechtliche Vorschriften gestellt. Diese Vorschriften wurden mit dem Ziel erlassen, Identitätsdiebstahl zu verhindern und Kundendaten besser zu schützen. Vergleichbare Sicherheitsverstöße liegen auch bei der Bekämpfung von Insiderdelikten vor.

Deshalb wäre es sinnvoll, die vorhandenen Instrumente zur Bekämpfung und Vermeidung von Insiderdelikten auch zur Erfüllung der Konformitätsanforderungen einzusetzen. Bislang ist dies mit den herkömmlichen Auditing-Verfahren nicht möglich gewesen. Doch durch Enterprise-Fraud-Management-Lösungen lässt sich dieselbe kontinuierliche Überwachung und Überprüfung jetzt auf die für den Nachweis der Konformität und Compliance notwendigen Maßnahmen übertragen. *(jp)*

Stephan Sippel ist Sales Manager Security & Integration Solutions, Zentral- und Osteuropa bei Attachmate.

Basiswissen IT-Sicherheit

Selbst für an IT-Sicherheit Interessierte scheint der Einstieg in den Dschungel der zahlreichen Sicherheitssysteme und der dahinter verborgenen Flut von Theoriebegriffen und Abkürzungen kein einfaches Unterfangen. An diesem Punkt möchte der Autor Werner Poguntke, der als Professor Angewandte Informatik und Mathematik an der FH Südwestfalen lehrt, ansetzen. Theoretisch ist auch der Einstieg in die Thematik, in dem der Schreiber die "Gefahren, Angriffe und Risiken" und damit den Begriff der IT-Sicherheit charakterisiert. Ohne sich hierbei übermäßig aufzuhalten, widmet er sich hiernach den kryptologischen Verfahren und Protokollen. So lernt der Leser diverse Verschlüsselungsverfahren wie DES, AES, RSA oder Hash-Funktionen kennen. Vom Informationsgehalt versucht der Autor sich populärwissenschaftlich den jeweiligen Verfahren zu nähern und die mathematischen Hintergründe auf ein Minimum zu reduzieren.

Das Folgekapitel ist etwas irritierend mit "Computersicherheit" betitelt und beinhaltet im Wesentlichen die Problematik Zugangs- und Zugriffskontrolle. Auf insgesamt nur 50 Buchseiten werden Passwortsicherheit, Biometrie, Kerberos sowie Viren und die Sicherheit von Betriebssystemen angerissen. Den Abschluss bildet das Kapitel "Sicherheit in Netzen". Hier geht der Autor kurz auf verschiedene Firewall-Systeme ein. Die Erläuterungen verschiedener Schichten auf Protokollebene (primär TCP/IP) sind für die potentielle Leserschaft vermutlich überfordernd, zumal die Ausführungen sehr knapp gehalten sind. Beim Thema E-Mailsicherheit verweist der Autor fast ausschließlich auf das PGP-Verfahren. Ein Glossar, Literaturempfehlungen und ein Sachindex schließen das Buch ab.

Fazit: Für Themenfremde ist das Werk sicherlich ein brauchbares Buch als Grobüberblick, ohne dabei zu überragen. Wer detailreichere Informationen sucht, wird den Weg über Sekundärquellen nicht umgehen können. Und trotz überarbeiteter Neuauflage wird im Kapitel über Browser nur auf ältere Modelle verwiesen – ein Manko, das bei einer Neuauflage etwas peinlich wirkt.

Frank Große

Autor:	Werner Poguntke
Verlag:	W3L-Verlag
Preis:	29,90 Euro
ISBN:	978-3-86834-021-1
Bewertung:	★★½☆☆

Microsoft Forefront Threat Management Gateway 2010

Der ISA Server ist Geschichte. Microsoft läutet mit dem Forefront Threat Management Gateway (TMG) seine neueste Sicherheitsgeneration ein. Mit Marc Grote, Christian Gröbner und Dieter Rauscher hat sich ein erfahrenes Autoren-Team für ein neues Referenzwerk dazu gefunden, das sich bereits seit dem ISA Server 2004 mit der Thematik auseinandersetzt. Im Wesentlichen ist das Buch in sechs Teile und einen Anhang untergliedert und wird dabei von einer in der Einleitung charakterisierten Beispielfirma begleitet. Im ersten Abschnitt "Grundlagen und Installation" führt das Autoren-Trio bislang wenig erfahrene Administratoren an die Thematik "Firewall" heran, ohne dabei zu theoretisch zu werden. Im Verlauf des Kapitels werden so die (neuen) Eigenschaften der Produktfamilie um TMG 2010 beschrieben.

Der zweite Teil des Buches umfasst zusammen mit dem Folgeteil und insgesamt 580 Seiten ein Kernstück des Gesamtinhalts. Hierbei wurde neben der Installation der Fokus auf die Konfiguration und Administration von TMG 2010 gelegt. So finden sowohl die grundsätzliche Netzwerkeinrichtung, Cache-Konfiguration und ISP-Redundanz als auch die Themen TMG-Clients und Zertifikatverwaltung Berücksichtigung. Der Schwerpunkt liegt jedoch auf dem Betrieb der Sicherheitslösung. Dabei erläutern die Autoren Zugriffsregeln, Veröffentlichungen von Exchange und Web (RADIUS, LDAP, Remotedesktops). Aber auch das Thema E-Mailschutz kommt nicht zu kurz, wenngleich der Fokus hier erwartungsgemäß auf Exchange Server 2010 liegt. Die Erläuterung der Anbindung von mobilen Computern, Heimarbeitsplätzen und Zweigstellen via VPN sind Aufgabe des nächsten Teils. Einer kurzen Einleitung zum Thema VPN folgt die Clientanbindung und Quarantänesteuerung. Den Standortverbindungen ist ein eigenes Kapitel gewidmet, ebenso der Enterprise Edition von Forefront TMG 2010.

Fazit: Das Buch richtet sich in erster Linie an Administratoren, die den Einsatz von Forefront TMG 2010 planen oder bereits vollzogen haben und technisch interessiert sind. Herausgekommen ist eine 900-seitige Bibel, die dem Anspruch eines Referenzwerkes vollauf gerecht wird.

Frank Große

Autoren:	Marc Grote, Christian Gröbner, Dieter Rauscher
Verlag:	Microsoft Press
Preis:	59,90 Euro
ISBN:	978-3-86645-127-8
Bewertung:	★★★★★

www.it-sicherheit.de

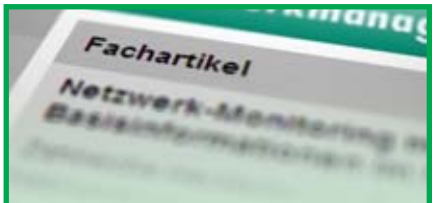
Rundum-Infopaket zur IT-Security

In kaum einem IT-Bereich ändern sich die Dinge so schnell wie im Security-Umfeld. Wöchentlich ist von neuen Trends und Angriffsmethoden zu lesen. Bislang als sicher geglaubte Systeme sind plötzlich verwundbar und das eigene Sicherheitskonzept muss schnellstmöglich angepasst werden. Für den Admin, der in kleineren Umgebungen meist noch jede Menge anderer Sorgen hat, ist es daher nicht leicht, den Überblick zu behalten. Gut, wer den "Marktplatz für IT-Sicherheit" kennt. Das "neutrale Portal" zur IT-Security wird vom Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen betrieben. Entwickelt wurde die nichtkommerzielle Webseite durch Studenten und wissenschaftliche Mitarbeiter der FH, um "Hilfestellungen im Bereich der IT-Sicherheit zu geben, damit moderne IT-Techniken und Dienste mit weniger Risiken verwendet werden können".

Mit über 1.000 eingetragenen Sicherheitsanbietern bezeichnet sich das Portal selbst als das bundesweit größte Verzeichnis in diesem Bereich sowie als die umfassendste Jobbörse im Sicherheitsumfeld Deutschlands. Aufgeteilt ist die Seite in die fünf Rubriken "Anbieter", "Produkte", "Veranstaltungen", "Ratgeber" und "Jobs". So finden Interessenten in der ersten Rubrik einen Überblick über relevante Hersteller von IT-Sicherheitsprodukten. Dazu gehört neben der Anschrift, E-Mailadresse und Telefonnummer auch die Info, in welchen Kategorien das Unternehmen tätig ist und wo die jeweiligen Kompetenzen liegen. Eine Suche nach frei wählbaren Begriffen sowie dem Ort helfen, den passenden Anbieter zu finden. Noch konkreter wird es in der Rubrik "Produkte". Hier können die Besucher gezielt nach Hardware, Software und Dienstleistungen suchen.

Eine Wolke aus Schlagworten listet jeweils die wichtigsten Suchbegriffe übersichtlich auf. Klickt der Besucher auf eines der angezeigten Produkte, erhält er neben einem Abbild auch eine informative Produktbeschreibung sowie die Kontaktdaten des Anbieters. Lediglich einen Preis sucht man vergebens – hier muss der Hersteller dann direkt Auskunft geben. Ein ähnliches Bild zeigt sich in der Rubrik "Veranstaltungen". Hier können Admins, ebenfalls nach Region und Schlagworten sortiert, das passende Event ausfindig machen. Unter "Ratgeber" finden sich zudem zahlreiche hilfreiche Artikel rund um das Thema Sicherheit, etwa wie sich Daten sicher speichern und löschen lassen oder welchen Schutz es vor Spam gibt. Die Rubrik "Jobs" schließlich rundet die Seite ab. So finden die Besucher in Kooperation mit verschiedenen Jobbörsen vielfältige Stellenangebote – beispielsweise über 1.000 aus den vergangenen 30 Tagen. *(dr)*

Auf it-sicherheit.de finden sich Security-Infos mit Hard- und Software-Angeboten, Dienstleistungen und Jobs



Unser Internetauftritt versorgt Sie wöchentlich mit einem interessanten Fachartikel. Diesen Monat erfahren Sie auf unserer Webseite mehr zu folgenden Themen:

Anwenderbericht: E-Mails rechtskonform archivieren und wiederherstellen

Die Unternehmensgruppe Dillenburger ist als Dienstleister im Bereich der technischen Gebäudeausrüstung tätig. Da die Suche nach älteren E-Mails einen enormen Zeitaufwand darstellte, war die Einführung einer automatisierten und rechtssicheren Lösung zur E-Mail-Archivierung nötig. Lesen Sie online, welche Faktoren auf der Suche nach einer neuen Software wichtig waren und wie sich die Lösung im täglichen Einsatz schlägt.
www.it-administrator.de/themen/kommunikation/fachartikel/92703.html

Verteidigungslinie gegen Spam

Quasi minütlich wird das E-Mail-Postfach mit Angeboten von Online-Casinos, Pillenverkäufern oder skurrilen Geschäftsideen aus Afrika gefüllt. In unserem Fachartikel im Web erklären wir, mit welchen Technologien sich Spam aktuell begegnen lässt, wer hinter den Millionen von Werbemails steckt und wie zukünftige Bekämpfungsstrategien aussehen könnten.
www.it-administrator.de/themen/sicherheit/fachartikel/92704.html

Sicherheit beim Cloud Computing

Cloud Computing ist derzeit in aller Munde – manche Unternehmen stehen der Wolke aufgrund von Sicherheitsbedenken jedoch noch immer skeptisch gegenüber. Zweifellos sind der Sicherheitsstatus in der Cloud und die Security-Verfahren, durch die sich SaaS-Dienstleister unterscheiden, für IT-Entscheider grundlegende Themen. In unserem Online-Beitrag helfen wir Ihnen mit einer Checkliste dabei, die besten Sicherheitskonzepte für die Cloud zu finden.
www.it-administrator.de/themen/sicherheit/fachartikel/92705.html

Den Anwender vor sich selbst schützen

Noch vor zwei Jahren war es Standard, die private Nutzung des Internets am Arbeitsplatz stark einzuschränken – diese Haltung ist heute von der Realität eingeholt: Wo sich in Facebook, Xing & Co. private und geschäftliche Nutzung kaum trennen lassen, ist eine Sperrung demotivierend oder gar kontraproduktiv. In unserem Web-Artikel gehen wir auf die Methoden ein, wie Sie trotz Web 2.0 und sozialen Netzwerken für Sicherheit im Unternehmen sorgen.
www.it-administrator.de/themen/sicherheit/fachartikel/92706.html

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

»Als Ausgleich zur Büroarbeit brauche ich frische Luft«

Torsten Stauber (33) arbeitet als IT-Administrator in verschiedenen IT-Umgebungen, die er als SAP-Consultant gemeinsam mit seinen Kunden entwickelt. Dabei betreut der Hobby-Heimwerker für die Würzburger TakeASP mit viel Engagement SAP-Projekte unterschiedlicher Größenordnung. Langweilig wird es ihm dabei nie.

Welche Aspekte Ihres Berufs machen Ihnen mehr und welche weniger Spaß?

Spaß macht mir, dass es immer wieder neue Produkte und Projekte gibt. Sei es im SAP-Umfeld, bei den Datenbanken sowie bei den Betriebssystemen. Das hält den Arbeitsalltag lebendig, weil ich mich immer aktuell informieren muss, denn durch die individuellen Anforderungen der Kunden bin ich gezwungen stets "up to date" zu sein. Weniger Spaß macht mir, dass meine Familie manchmal darunter leidet, dass ich auch abends oder am Wochenende arbeiten muss, wenn Projekte das verlangen.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Aktuell ist die Virtualisierung von SAP unter SLES mit XEN sowie die Einführung von Netweaver 7.3 eine Hauptaufgabe. Darüber hinaus steht bei einigen Kunden die Migration von SAP-Systemen, bei anderen ein Upgrade an.

Mit welcher aktuellen IT-Technologie würden Sie gern einmal arbeiten?

Ein intensives Arbeiten mit den verschiedenen Möglichkeiten des Cloud Computing würde mich sehr reizen.

Wie denken Sie, arbeitet ein Administrator in zehn Jahren?

Ich denke, unser Job wird kaum anders sein als heute oder als vor zehn Jahren. Einzig der Arbeitsort wird noch flexibler. Waren wir früher eher an einem festen Büroplatz mit Netzanbindung tätig, können wir heute von fast überall auf die Systeme zugreifen. Die moderne Kommunikation über Handy, Internet, WLAN macht dies möglich.

Warum würden Sie einem jungen Menschen raten, Administrator zu werden?

Ich denke, IT-Administrator ist nach wie vor ein Job mit Zukunft. Es gibt immer die Möglichkeit, Neues zu lernen und der Arbeitsalltag ist niemals langweilig.

Mit welchen Techniken gewährleisten Sie die Sicherheit Ihrer Unternehmensdaten?

Sensible Daten werden natürlich verschlüsselt. Darüber hinaus setzen wir Firewalls und andere Sicherheitsmechanismen ein. Hinzu kommen individuelle Berechtigungskonzepte und weitere projektbezogene Maßnahmen, über die wir allerdings nicht öffentlich sprechen.

Wie beurteilen Sie die Sicherheit von Unternehmensdaten im Zusammenhang mit der Cloud?

Generell finde ich das Thema Cloud Computing als Option sehr interessant, wobei ich denke, dass unternehmenskritische Daten spezieller Sicherheitsmaßnahmen bedürfen. Und ob die Cloud bei jeder Art von Daten das richtige Umfeld ist, sei dahingestellt und muss individuell entschieden werden. Die wichtigste Frage bleibt: Wie sicher sind meine Daten in der Cloud und kann ich jederzeit darauf zugreifen?

Wie finden Sie den nötigen Ausgleich zu Ihrer Arbeit?

Da ich überwiegend im Büro arbeite, brauche ich zum Ausgleich frische Luft. In der Regel heißt das: raus aus den vier Wänden. Sport und Spaziergänge helfen mir, den Kopf frei zu bekommen.

Nehmen Sie Ihre Arbeit auch mit in den Urlaub oder ins Wochenende?

Ja, das passiert schon oft. In meinem Job lässt sich das aber nicht vermeiden, denn ich fühle mich für die Projekte meiner Kunden verantwortlich. Da kann man nicht einfach den Stift fallen lassen und gehen.

Inwieweit hat Ihr Beruf Ihre Hobbys geprägt?

Meine eigenen PCs habe ich mir schon immer selbst zusammengebaut. Ansonsten bin ich in meiner Freizeit auch öfter einmal im Internet unterwegs, um Informationen zu meinen Interessensgebieten zu finden.

Geburtstag: 07.10.1977
Familienstand: verheiratet
Hobbys: handwerkliche Tätigkeiten, Snowboarden, Astronomie, Computer

Torsten Stauber, IT-Administrator

Ausbildung
- Ausbildung zum Kommunikationselektroniker bei der Deutschen Telekom
- Nach und nach immer mehr in der IT-Administration tätig
- Heute Senior Consultant für SAP-Lösungen

Betreute IT-Infrastruktur
- Betreuung von unterschiedlichen Umgebungen
- Spektrum von kleinen SAP Einzelsystemen bis zur großen Kundenlandschaft mit komplexen Anwendungen wie ERP oder anderen Applikationen
- Systemmanagement-Werkzeuge kundenabhängig von Nagios und Tivoli bis hin zum SAP Solution Manager

Sind Sie auch in Ihrem Freundes- und Bekanntenkreis als IT-Supporter gefragt?

Als gelernter Kommunikationselektroniker werde ich immer noch angesprochen, wenn es im Umfeld von Telefon und Internet Fragen gibt. Wobei sich hier die Technik mittlerweile so verändert hat, dass ich keinen aktuellen Überblick mehr habe und nicht immer helfen kann.

Das Interview führte Petra Adamik.

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

Was haben Sie zu sagen?

Die Ausgabe 3/11 erscheint am 1. März 2011

Schwerpunktthema:

Netzwerkmanagement

Im Test: Ipswitch WhatsUp Gold 14.3

Im Test: LANDesk Management Suite 9

Workshop: Netzwerkanalyse mit dem Nagios-Nachfolger Shinken

Workshop: Fehlersuche im Ethernet

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

Unsere Ausgabe im **April** steht unter dem Schwerpunkt **Backup & Recovery**. In unseren Tests nehmen wir unter anderem Veeam ESX Backup 5.0 unter die Lupe. In den Workshops lesen Sie, wie das Backup & Recovery eines Hyper-V Hosts funktioniert und Sie ein Bare Metal Recovery von Windows Server 2008 durchführen.

Als Schwerpunkt im **Mai** folgt dann das Thema **Server-based Computing**.

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

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

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

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

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

Autoren dieser Ausgabe
Petra Adamik, Sandra Adelberger, Thomas Bär, Sascha Giebelhausen, Frank Große, Thomas Joos, Martin Kuppinger, Robert Lindermeier, Hendrik Pilz, Dr. Holger Reibold, Thorsten Scherf, Stephan Sippel, Betram Wöhrmann

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

Es gilt die Anzeigenpreisliste Nr. 7 vom 01.11.2009

LAC/2008

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

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

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

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

Erscheinungsweise
monatlich

Bezugspreise
Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-
Jahresabonnement Inland mit Jahres-CD: € 144,84
Studentenabonnement Inland mit Jahres-CD: € 77,34
Jahresabonnement Ausland mit Jahres-CD: € 159,84
Studentenabonnement Ausland mit Jahres-CD: € 84,84
All-Inclusive Jahresabo
(mit Sonderheften + Jahres-CD) Inland: € 184,64
All-Inclusive Studentenabo Inland: € 117,14
All-Inclusive Jahresabo Ausland: € 199,64
All-Inclusive Studentenabo Ausland: € 124,64
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.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
80802 München
Tel.: 089/4445408-0
Fax: 089/4445408-99
(zugleich Anschrift aller Verantwortlichen)
Web: www.heinemann-verlag.de
E-Mail: info@heinemann-verlag.de
Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

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

ISSN
1614-2888

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

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

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

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

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

INSERENTENVERZEICHNIS
Die Ausgabe enthält eine Teilbeilage der Firma balesio AG.

Das IT-Administrator Komplettprogramm!!!

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

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

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

Als bestehender Jahresabonnent können Sie hier upgraden:

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

Oder Sie sind Neukunde? Hier können Sie bestellen:

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

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

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

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

Warum die DLRG dank Fujitsu nicht in Datenfluten untergeht ...

PUSH YOUR BUSINESS

Wir sind dabei! Besuchen Sie uns:
1. – 5. März 2011 Hannover

Halle 2, B38 Fokus Cloud
Halle 9, C60 Public Sector Parc
Halle 15, F15 Planet Reseller

CeBIT

http://de.fujitsu.com/cebit

»Dank Virtualisierung und den stabilen Systemen von Fujitsu läuft unsere IT sicher und mit überragender Performance. Wir haben den großen Wurf gewagt – und gewonnen.«

Frank Rabe, Leiter IT der DLRG

Wie macht man Lebensrettern das IT-Leben leichter und wirtschaftlicher? Indem man sie vor den Datenfluten rettet, die über eine Million aktive Mitglieder und Förderer verursachen. So geschehen bei der Deutschen Lebens-Rettungs-Gesellschaft, mit einer Kombination aus PRIMERGY Servern und ETERNUS Speichersystemen von Fujitsu. Wo zuvor in die Jahre gekommene Technik den Kosten Druck und den Administratoren Frust bereitete, leitet nunmehr das virtuelle Zusammenspiel leistungsstarker und innovativer Fujitsu-Technologie den Fluss von Daten und Prozessen – und das ohne Frustfaktor für Budget und Administration.
http://de.fujitsu.com/referenzen-in-deutschland

shaping tomorrow with you

FUJITSU