konradin MEDIENGRUPPE

www.windowsitpro.de

10/2006

Windows IT Pro

Das Magazin für den Windows-Administrator

Sicherheitsstrategien und -lösungen

DNS-Server richtig verwalten
Sicheres Single-sign-on
Angriffspunkte fest im Griff

LAB-REPORT:

- Praxistest: Doppelte Speicherdichte
- E-Mail-Appliance im Einsatz
- FTP-Client

SPECIAL:

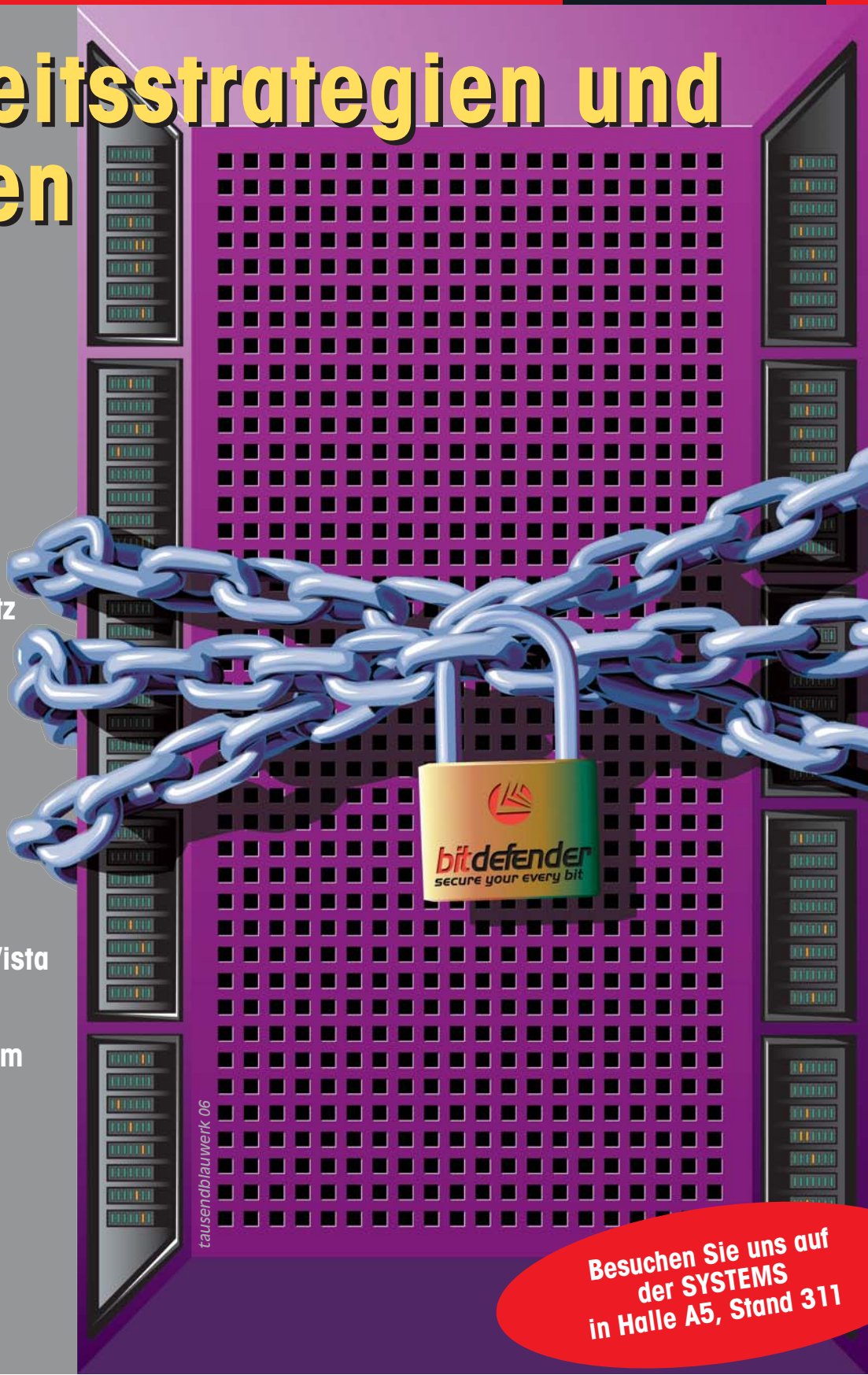
- Sicheres Drucken im Netz
- WSH hilft Konfigurieren

TOOLKIT:

- Software Lifecycle unter Vista
- Datenverstecke aufspüren
- Windows-Systemdienste im Skript

Marktübersicht

NAS-Lösungen



Absicherung von Laptops und Notebooks

Persönlich, virtuell und sicher

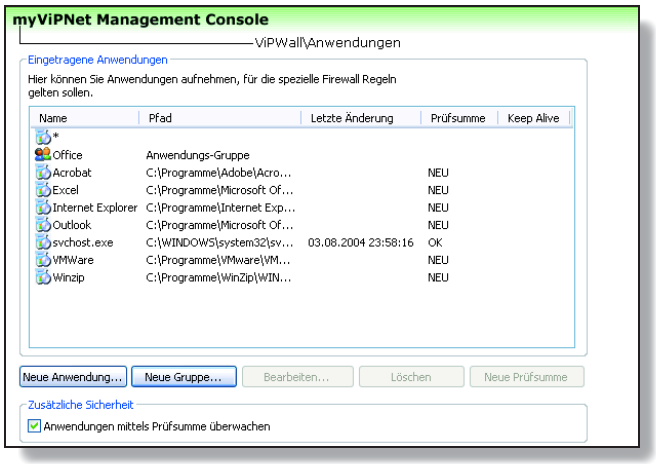
von Thomas Kleibömer

Es existiert wohl kaum noch ein Netzwerk, in dem nicht mobile Mitarbeiter von außen auf firmeninterne Daten und Anwendungen zugreifen. Um die damit verbundenen Sicherheitsprobleme in den Griff zu bekommen, bietet sich der Einsatz einer Sicherheitslösung an, wie sie hier vorgestellt wird.

Immer mehr Mitarbeiter erledigen ihre Aufgaben an verschiedenen Firmensitzen, vor Ort beim Kunden oder von zu Hause aus. Diese Telearbeiter finden dann verschiedene Infrastrukturen vor und auch ihre Anbindung ans Internet erfolgt über unterschiedliche Zugänge. Trotzdem soll dabei der Zugriff auf zentrale Dienste jederzeit völlig transparent und möglichst ohne lästigen Konfigurationsaufwand erfolgen. Zugleich muss der Rechner an jedem Einsatzort vor unerlaubtem Zugriff geschützt sein, und es sollten nur die jeweils benötigten Anwendungen und Netzwerkzugriffe zur Verfügung stehen.

Verschiedene Standorte: Regeln und Berechtigungen sind gefordert. Zunächst muss der Administrator die Möglichkeit haben, für die verschiedenen Standorte entsprechende Regeln und Berechtigungen zu hinterlegen. Darüber hinaus muss das System in der Lage sein, die Standorte und die verfügbare Netzwerkinfrastruktur automatisch zu erkennen. Bei der Vielzahl der heutigen Anwendungen und Dienste ist es fast unmöglich, sich sämtliche Zugangsdaten zu merken. Diese wichtigen Daten aber zu speichern oder gar auf einem Notizzettel zu notieren ist sehr riskant und sicher nicht empfehlenswert.
Im Idealfall hat der Anwender seine Zugangsdaten in einem sicheren Passwortspeicher hinterlegt, der sich überall mitnehmen und einsetzen lässt, jedoch nicht integraler Bestandteil des Computers ist. Authentifizierung am System, an beliebigen Anwendungen und Internetdiensten erfolgen in diesem Fall automatisch und komfortabel. Bewährt hat sich dafür der so genannte „Crypto-Token“, beispielsweise für die USB-Schnittstelle. Der Benutzer braucht sich am Token nur einmal beim Einstecken ins mobile Arbeitsgerät zu authentifizieren. Fällt der Computer dann doch in fremde Hände, so muss sichergestellt sein, dass Unberechtigte unter keinen Umständen auf die gespeicherte Daten zugreifen können, über VPN-Verbindungen ins Firmennetz gelangen oder über gespeicherte Anmeldedaten Zugriff auf Anwendungen erhalten.
Um all diese Anforderung zu erfüllen, kann ein VPN in Verbindung mit einem USB-Token zum Einsatz kommen. Das hier vorgestellte myViPNet VPN bietet noch die Möglichkeit, mehrere VPN-Verbindungen gleichzeitig zu betreiben und diese jeweils automatisch bei Bedarf zu öffnen. Dies geschieht unabhängig vom benötigten VPN-Verfahren der jeweiligen Gegenstellen. Ebenso können pro VPN verschiedene diskrete Zielnetze konfiguriert werden. Die Lösung ist aufgrund ihrer Implementierung in der Lage, den Netzwerkverkehr zu kontrollieren und somit das Routing innerhalb der Netzwerkschicht und zwischen den VPNs zu übernehmen.
So hat der Administrator die Möglichkeit, je nach Standort automatische Profile über unterschiedliche VPN-Verbindungen bereitzustellen. Die VPN-Protokolle IPSec und com2-VPN sind hier so implementiert, dass die Lösung auch Network Address Translation (NAT) problemlos verwenden kann. Als Gegenstellen für die Einwahl in der Zentrale oder weiteren Standorten dient die Routerlösung „Gateland“, die wahlweise mit dem proprietären nicht veröffentlichten com2-VPN-Protokoll oder auch mit dem offenen Standard IPSec betrieben werden kann.

Die Sicherheit erhöhen: Komplette Konfiguration speichern. Um eine höhere Sicherheit zu erreichen, hat der Administrator die Möglichkeit, direkt aus der Konfiguration heraus die komplette VPN-Konfiguration per Mausklick auf dem so genannten „ViPKey“ abzuspeichern. So kann sicherstellen, dass diese Einstellungen auch bei Verlust des Rechners nicht offen liegen. Zieht der Anwender dieses USB-Token dann von seinen Rechner ab, so ist auch die VPN-Verbindung inklusive aller Zugangsdaten nicht mehr zugänglich.
Ein weiterer wichtiger Sicherheitsaspekt ist eine Firewall, die bei dieser Lösung ebenfalls zur Verfügung steht. Die so genannte „myViPNet“-Firewall erlaubt es, individuell für jeden Netzwerkadapter und für jedes VPN abhängig vom Standort Zugriffe auf Protokoll-, Port- und Anwendungsebene in ein- und ausgehender Richtung zu regeln. Auch hier hat der Administrator die Option, das entsprechende Regelwerk für die Firewall entweder zentral über den „Config Server“, der zur zentralen Konfiguration aller Clients dient, oder aber vor Ort direkt am Rechner des Anwenders zu konfigurieren. Zudem kann er einen Lernmodus aktivieren, der bei noch nicht konfigurierten Zugriffen den Anwender um Erlaubnis für diesen Zugriff fragt. Dabei wird sämtlicher Netzwerkverkehr auf Device-Treiber-Ebene kontrolliert. Durch die Anwendungsüberwachung ist zudem sichergestellt, dass nur gewünschte Applikationen



Keine Sicherheit ohne Firewall: Die Firewall-Regeln für Ports, Dienste und Applikationen werden bei der vorgestellten Lösung in Containern gespeichert und können dann unterschiedlichen Profilen und Adaptern zugeordnet werden. (Quelle: com2)

wie zum Beispiel Outlook Zugriff auf das Netzwerk erhalten und die Anwendung nicht manipuliert werden kann.

Ging es bei diesen Maßnahmen vor allen Dingen darum, unberechtigte Zugriffe auf die Unternehmensdaten zu verhindern, dient die Komponente „ViPDrive“ dazu, sensitive Daten auf dem System in einem verschlüsselten virtuellen Laufwerk abzulegen oder auch vollständige Festplattenpartitionen zu verschlüsseln. Der Administrator hat dabei auch die Möglichkeit, beide Verfahren miteinander zu kombinieren. Wenn der Anwender auf die Daten zugreifen möchte, verlangt die Lösung neben dem auf dem USB-Token gespeicherten Schlüssel auch, dass dieser Token selbst zugelassen ist. Das bedeutet, dass er zunächst durch seine eindeutige ID identifiziert werden muss, ehe das System den Zugriff ermöglicht. Diese Komponente verwendet eine sektorbasierte Verschlüsselung, die im so genannten „Cipher Block Chaining Mode“ (CBC) arbeitet. Der Einsatz dieses Verfahrens gewährleistet das Erzeugen unterschiedlicher Chiffren auch bei gleichen Ursprungsdaten. Zur optimalen Ausnutzung des theoretisch möglichen Chiffreraums werden so genannte „Salting“- und Hash-Verfahren verwendet. Diese Verfahren erschweren potenziellen Angreifern zusätzlich das Leben, indem bei jeder Verschlüsselung einer der implementierten Hash-Algorithmen (beispielsweise SHA-1, SHA-256, MD5 oder RIPEMD) willkürlich ausgewählt wird. Als Verschlüsselungsalgorithmen verwendet der Hersteller Triple-DES, AES-256 und Blowfish. Sie arbeiten mit Schlüssellängen von 168, 256 und 448 Bits und bieten eine vergleichbare Sicherheit bei unterschiedlicher Geschwindigkeit. Das System arbeitet in diesem Fall mit virtuellen Laufwerken oder Containern. Das sind Dateien, die wie ein Festplatten-Image den Inhalt eines Laufwerks repräsentieren. Wird eine solche Datei mit dem oben beschriebenen Verfahren verschlüsselt, bleibt das dargestellte Laufwerk ohne die Kenntnis des Schlüssels unsichtbar und vor fremden Augen geschützt. „myViPNet“ unterstützt sowohl NTFS als auch FAT32-Container. Wer für seine Datencontainer ein NTFS-Dateisystem einsetzt, kann auch nachträglich die Größe des jeweiligen Containers verändern. Entscheidet sich der Administrator hingegen dafür, gleich die Partitionsverschlüsselung einzusetzen, so wird auch das Betriebssystem chiffriert. Für den Start eines derart verschlüsselten Systems wird eine so genannte „Pre-Boot“-Authentifizierung benötigt. Die Software schaltet dann dem eigentlichen System-Loader ein Programm vor, das nach Erhalt des Schlüssels die Partition entsperrt und die Daten wieder dechiffriert. So kann der Systembetreuer sicherstellen, dass ein derart verschlüsselter Computer ohne das richtige Kennwort nicht mehr gestartet werden kann. Da es aber durchaus vorkommt, dass dieses Kennwort verloren geht, kann zusätzlich auch ein zweiter Schlüssel für diese Partition angelegt werden. Mit Hilfe dieses Schlüssels ist der Administrator notfalls in der Lage, ein zeitlich begrenztes Kennwort zu erzeugen. Mit dessen Hilfe lässt sich der betreffende Rechner innerhalb eines begrenzten Zeitraums wieder starten, sodass Daten gerettet werden können. *(fms)*

Der Autor:

Thomas Kleibömer ist Geschäftsführer der Firma com2 in Hallbergmoos bei München.

Marktübersicht NAS-Systeme

Viel mehr Speicher

Man kann eigentlich nie so viel Speicherplatz haben, als dass er nicht irgendwann (in der Regel viel früher als es sowohl Anwender als auch Systembetreuer erwartet haben) wieder nicht ausreicht. Eine Lösung, um den Speicherplatz im Unternehmensnetz zu erweitern, besteht darin so genannte NAS-Systeme zu verwenden. Wie groß das Interesse an NAS-Systemen wirklich ist, konnten wir bei der Bearbeitung dieser Marktübersicht schnell feststellen: Wir wurden von einer waren Flut an Rückmeldungen überrascht, sodass wir nicht alle Informationen hier im Heft abdrucken können. Deshalb finden Sie hier in der Windows IT Pro eine gekürzte Marktübersicht, in der alle NAS-Anbieter, die auf unseren Aufruf reagiert haben, mit jeweils einem System vertreten sind. Die komplette Übersicht mit allen Systemen und allen Modellen finden Sie dann im Internet als PDF-Datei zum Download unter der folgenden URL:

`http://www.netigator.de/netigator/live/nt_mue/liste.html?obj=WM&np=markt`

NAS-Lösungen

		Betriebssysteme				Hardware										Sicherheit						Funktionen
						Prozessor																
Hersteller/ Anbieter Telefon	Produktname (Hersteller)	Windows Storage Server 2003	Linux-basierend	Unix-basierend	Andere Betriebssysteme	Hauptprozessortyp	CPU-Anzahl	Taktfrequenz CPU	Max. Arbeitsspeicher-Ausbau	Hard-Disk-Interface	Max. Anzahl Festplatten	Max. Kapazität	Anzahl NICs	NIC-Geschwindigkeit	Rackmounting-fähig	Unterstützte RAID-Level	Redundante Netzteile	Redundante Lüfter	Hotswap fähige Festplatten	Hotspare definierbar	Automatische Benachrichtigung im Schadensfall	Zusatzfunktionen
ARP Datacom 06074/491105	Harddisk-Server CL-NAS 200 (Claxan)		●			MIPS	1	200 MHz	32 MB	IDE	1	500 GB	1	10/ 100 TX	Nein						ja	2x USB-Port: Prinserver, Massenspeicher; UPnP AV MediaServer; NFS-Protokoll; HTTP-Webserver; FTP-Server
Adaptec 089/82088984	Snap Server 520		●			AMD	1	2,2 GHz	4 GB	SATA 2	4	2 TB	2	1 GB	Ja	0,1,5	●	●	●	●	ja	Backup SW & Antivirus
Adaptron 08141/34750110	Base-NAS 3000		●			Xeon	1–2	3,6 GHz	16 GB	SATA 2	16/ 32	24 TB	2–6	1/10 GB	Ja	0,1,5,10	✓	●	●	●	ja	integrierte Backup-Clients
Atix 089/121409–51	com.oonics NASBox		●			x86	1	3,0 GHz	8 GB	SATA/ SCSI	14	6,1 TB	2	6 GB	ja	0,1,5	●	●	●	●	ja	
Buffalo Techn. 0211/3611790	TS-TGL IR5		●				1			SATA	4	2 TB	1	10/ 100/ 1000		1,5, JBOD					ja	FTP Server
Computer Business Center 069/97377252	DL380G4 Storage Server (HP)	●				Intel	2	3,4 GHz	8 GB	Ultra 320	4	1,2 TB	2	100/ 1000	Ja	0,1,5,10	●	●	●	●	ja	
Contra 3000 089/8544575	KMU Midrange NAS		●			P4	1	3 GHz	16 GB	SATA/ SCSI	24	18 TB	1–8	10/ 100/ 1000	Ja	0,1,5,10, 50,0+1	●	●	●	●	ja	
DA&S 07240/943215	StroTrends 1100 (AMI)		●			P4	1	3 GHz		SATA 2	4	2 TB	2	1 GB	Ja	0,1,5		●	●	●	l	

Informationen und Weblinks finden Sie unter www.windowsitpro.de/Marktübersicht

NAS-Lösungen

Hersteller/ Anbieter Telefon	Produktname (Hersteller)	Betriebssysteme				Hardware										Sicherheit						Funktionen
						Prozessor																
		Windows Storage Server 2003	Linux-basierend	Unix-basierend	Andere Betriebssysteme	Hauptprozessortyp	CPU-Anzahl	Taktfrequenz CPU	Max. Arbeitsspeicher-Ausbau	Hard-Disk-Interface	Max. Anzahl Festplatten	Max. Kapazität	Anzahl NICs	NIC-Geschwindigkeit	Rackmounting-fähig	Unterstützte RAID-Level	Redundante Netzteile	Redundante Lüfter	Hotswap fähige Festplatten	Hotspare definierbar	Automatische Benachrichtigung im Schadensfall	Zusatzfunktionen
EDV Support 06028/9912-0	Open-E-NAS-XSR (Open-E)		●				32		64 GB				12	1 GB	Ja						ja	Backup-Agenten, Antivirus u.a.
Eurostor 0711/70709170	ES-2000-NAS	●				P4	1	3 GHz	1 GB	SATA 2	16	6,4 TB	2	10 GB	Ja	0,1,3,5,6	●	●	●	●	ja	
Exus-Data 04795/9571300	OSA 4		●			P4	1	3 GHz	4 GB		4	2 TB	2	10/ 100/ 1000	Ja	0,1,10,5,6			●	●	ja	Backup-Agenten, Antivirus u.a.
Fujitsu Siemens 089/32224458	FibreCAT N20i	●				P Dual	1	3,0	2 GB	SATA	4	2 TB	2	1000	Ja	1,5	●	●	●	●	ja	Printserver
Glöckner & Lauer 0731/974010	NAS-XSR (Open-E)		●			Intel	32		64 GB	DIE/ SCSI/ SATA	opt.	opt.	12	1 GB/ 10 GB	Ja	opt.	●	●	●	●	ja	Backup-Agenten, Antivirus u.a.
IP & S 0041/794070563	Open-E (Open-E)		●		Open-E		2		1,2 TB	SATA 2	6	900 GB	2	1 GB	Ja	5,1-0	●	●	●	●	ja	Printserver
Longshine 04102/4922-0	LCS-8220		●			MSA2 006	1	170 MHz	64 MB	IDE	1	400 GB	1	100 MBS								Web-Server, FTP-Server, Bittorrent-Client
N-Tec 089/958407-22	rapidNAS SR104-S2		●			P4 630	1	3,0 GHz	8 GB	SATA 2	4	3 TB	2	10/ 100/ 1000	Ja	0,1,3,5,6		●	●	●	ja	
Pillar 089/90405486	Axiom 500				eigenes Echtzeit-betriebs-system	Intel	6-18	2,4 GHz	96 GB	SATA/ FC	832	387 TB	4-16	10/ 100/ 1001	Ja	5,0,1	●	●	●	●	ja	Worm FS im Standard und im Compliance-Mode
Plasmon Data 08751/875100	SNAZ S12-400		●			P4	1	3,4 GHz	2 GB	SATA	36	18 TB	4	Gb Ether-net	Ja	5,0,1	●	●	●	●	ja	Bakbone Netvault v.7.4 Workgroup, Backup Server incl VTZ
RubyTech 02252/950103	RubyStorage 1.6				WinXP Prof.	AMD Athlon 64	1	1800 MHz	4096 MB	SATA 300	4	1,6 TB	1	1000 MB/s		0,1,5,10					ja	Media Streaming Server, Video+Musik, Web+FTP-Server, Printserver
SSE 0041/79-6783245	SSE-NAS-Server (SSE+Open-E)		●			Intel	1	3,6 GHz	4 GB	SATA	24	18 TB	2x1 GB	1 GB	Ja	0,1,5,6	●	●	●	●	ja	Cross-Daten-Sychronisierung, Snapshot-Erstellung mit Zeitsteuerung, lokale Backups, Backup-Agents, Antivirenschutz, Überwachung, UPS- & Online-Kapazitätserweiterung Unterstützung
Stor IT Back 04185/707850	Storage Gateway 9200 (Reldata)		●			P4 Xeon	2	3,0 GHz	2 GB	SCSI/FC	extern	extern	6	10/ 100/ 1000	Ja	1,4,5	●	●			ja	Snapshot, NDMP-Sicherung, Storage-Virtualisierung, Cluster-Support, Replizierung
TIM 0611/2709-0	FAS 6000 (NetApp)				Data Ontap	Xeon	8		64 GB	SATA/ FC	1008	504 TB	32	10/ 100/ 1000	Ja	4+DI	●	●	●	●	ja	
Thomas Krenn 08551/915075	Storage Server 2003 R2 (Microsoft)	●				Premium D920	1	2,8 GHz	8 GB	ARC-1160	15	7,5 TB	2	1000 Mbit Ether-net	Ja	0,1,10,5, 6,JBOD	●	●	●	●	ja	Printserver

Informationen und Weblinks finden Sie unter www.windowsitpro.de/Marktübersicht

Vorschau

11/2006

Fokus: System- und Netzwerkmanagement

Viele der täglichen Aufgaben in der System- und Netzwerkverwaltung eines Windows-Netzwerks und der darin aktiven Systeme werden nach wie vor mit „einfachen" Shell-Skripten geregelt. Häufig kommen hier Skriptlösungen zum Einsatz, für die bereits die Bezeichnung „historisch" gelten könnte: In einem ausführlichen Artikel stellt ein Systemspezialist im Rahmen unseres Schwerpunktthemas in der Novemberausgabe der Windows IT Pro die zehn wichtigsten Richtlinien für das problemlose Arbeiten mit diesen „Command Shell Scripts" vor.

Lab-Report:

Wer kennt die Prozesse, zählt ihre Namen? Diesen Stoßseufzer werden wohl viele Systemverwalter schon von sich gegeben haben, wenn sich ein System nicht so verhält, wie man es von ihm verlangt und erwartet. Natürlich gibt es „Windows-Bordmittel" wie den Taskmanager, mit dessen Hilfe man schon ungefähr sagen kann, welche Programme samt ihrer Bibliotheken auf dem Windows-Rechner aktiv sind. Für unsere Rubrik Lab-Report in der Ausgabe 11/2006 der Windows IT Pro haben wir uns eine Software angesehen, deren Leistungsspektrum weit über das des Taskmanagers hinausgeht und verspricht, wirklich alle Prozesse zu kennen.

Toolkit:

Vom Systemadministrator zum einfachen Anwender: An dieses Gefühl werden sich noch viele Systemprofis gewöhnen müssen, wenn sie dann einmal vermehrt Systeme verwenden, die als Betriebssystem Windows Vista verwenden. UAC – User Account Control – heißt das Zauberwort, das nicht nur für Begeisterung sorgt. Für die nächste Ausgabe der Windows IT Pro haben unsere amerikanische Kollegen einen Blick auf diese Technik geworfen und versprechen Einblicke in die Vista-Sicherheit.

Themenänderung aus aktuellem Anlass vorbehalten

Die nächste Ausgabe der Windows IT Pro erscheint am 10. November 2006

Impressum

ISSN 1862-8222

Herausgeberin: Katja Kohlhammer
Verlag: Konradin IT-Verlag GmbH, Ernst-Mey-Straße 8, 70771 Leinfelden-Echterdingen

Geschäftsführung: Katja Kohlhammer, Peter Dilger

Verlagsbereichsleiter: Joachim Bettinger

Verlagsleitung : Rainer Huttenloher (Redaktion, Online)

Chefredaktion: Frank-Michael Schlede (fms), verantwortlich für den redaktionellen Inhalt, Tel. (089) 4 56 16-2 21

Autoren dieser Ausgabe: Oliver Bendig, Mark Burnett, Jan de Clercq, Jeff Fellinge, Margarete Keulen, Matthias Kirchhoff, Thomas Kleinbömer, Birgit Klinner, Michael Naunheim, Stuart Rauch, Bill Stewart

Ständige Mitarbeiter: Klaus Jotz (kj), Thomas Bär (tb), Susanne Franke (sf), Dr. Holger Schwichtenberg

Redaktionsassistenz: Nicky Amann, Tel. (089) 4 56 16-2 21
Fax: (089) 45616-100, nicky.amann@konradin.de

Layout: Michael Berwanger/Tausendblauwerk, Tel. (0 81 33) 939 800

Redaktionsanschrift:
Bretonischer Ring 13, 85630 Grasbrunn,
Fax (0 89) 4 56 16-1 00, www.windowsITPro.de

Anzeigenverkauf:
Anzeigenleitung:
Josef Kindsmüller, Tel. (0 89) 4 56 16-1 13
Fax (0 89) 4 56 16-2 50,
E-Mail: Josef.Kindsmueller@konradin.de
Anzeigenassistenz: Gabriele Fischböck,
Tel. (0 89) 4 56 16-2 62
Bretonischer Ring 13, 85630 Grasbrunn
Fax (0 89) 4 56 16-2 50
Anzeigenpreise: Zurzeit gilt Anzeigenpreisliste Nr. 14 vom 1.10.2005
Anzeigenservice: Andrea Haab,
Tel. (07 11) 7594-320

Erscheinungsweise: monatlich

Leserservice:
Marita Mlynek, Tel. (0711) 7594-302, Fax (0711) 7594-1302,
E-Mail: marita.mlynek@konradin.de

Bezugspreise: Einzelpreis € 6,00
Jahresabonnement Inland € 64,20 inkl. Versandk. und Mwst.
Ausland € 76,20.
Vorzugspreise: 50,40 € (Inland), 62,40 € (Ausland) für Studenten, Schüler, Auszubildende und Wehrpflichtige – nur gegen Nachweis.

Bezugszeit: Das Abonnement kann erstmals vier Wochen zum Ende des ersten Bezugsjahres gekündigt werden. Nach Ablauf des ersten Jahres gilt eine Kündigungsfrist von jeweils vier Wochen zum Quartalsende. Bei Nichterscheinen aus technischen Gründen oder höherer Gewalt entsteht kein Anspruch auf Ersatz.

Sonderdruckdienst: Alle in dieser Ausgabe erschienenen Beiträge sind in Form von Sonderdrucken erhältlich.
Kontakt: Josef Kindsmüller, Tel. (0 89) 4 56 16-1 13,
Fax (0 89) 4 56 16-2 50,
E-Mail: Josef.Kindsmueller@konradin.de.

Bank: BW Bank Stuttgart, Konto 2245849, BLZ 600 501 01

Gekennzeichnete Artikel stellen die Meinung des Autors, nicht unbedingt die der Redaktion dar. Für unverlangt eingesandte Manuskripte keine Gewähr.

Druck: Konradin Druck GmbH, Leinfelden-Echterdingen
Printed in Germany.

konradin MEDIENGRUPPE

ivw

LAC Business 2005

Mitglied der Leseranalyse Computerpresse 2005