IT-ADMINISTRATOR.DE

12/2011

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

System- und Plattformsicherheit

4 196583 212605 12

FÜR EIN SICHERES GEFÜHL!

Professionelle InterNetX Server-Lösungen.

Wir entwickeln mit Ihnen Ihr Sicherheitskonzept und stellen individuell konfigurierte Server bereit.

- 24/7 Support durch geschulte Techniker
- Zertifiziertes Tier 3 Data Center
- 1 GBit/s Uplink ohne Begrenzung pro Server
- Nur Markenhardware von DELL®, CISCO®, AMD®

Jetzt informieren:
www.internetx.eu

.eu Your European Identity DOMAINS GRATIS*

DELL OPTERON PROCESSOR AMD

InterNetX

www.internetx.eu

*Das Angebot richtet sich nur an Gewerbetreibende und kann in der Zeit vom 1.10. bis 31.12.2011 über www.internetx.eu bestellt werden. Die Domain-Registrierung betrifft ausschließlich .EU-Neuregistrierungen (bis zu 10 Domains gratis) für das 1. Jahr. Die Policies der Registry EURid sind maßgeblich. Weitere Informationen unter: www.internetx.eu

EDITORIAL

Botnet auf Kaperfahrt

Liebe Leser,

zwei Jahre ermittelte das FBI, dann klickten die Handschellen: Anfang November nahm die US-Behörde sechs Esten fest, denen der Aufbau eines Botnet vorgeworfen wird. Schon seit 2007 soll dieses Netzwerk weltweit aktiv gewesen sein und vier Millionen Rechner infiziert haben – allein in den USA ist von 500.000 befallenen PCs die Rede. Mittels der Schadsoftware "DNS Changer" gelang es den Kriminellen, die kompromittierten Computer zu kapern. Durch die Umleitung auf Werbeseiten und die Einblendung manipulierter Suchergebnisse sollen die Betrüger so mindestens 14 Millionen US-Dollar ergaunert haben. Die Malware verfügt zudem über gut ausgebaute Verteidigungslinien und verhindert erfolgreich die Aktualisierung von IT-Sicherheitslösungen.

Selbst wenn die Server zur Steuerung des Botnet mittlerweile offline sind – die Malware ist auf den betroffenen Rechnern weiterhin aktiv und macht diese durch ausgehebelte Sicherheitsfunktionen zum Einfallstor für andere Schädlinge. Auch in Unternehmensnetzwerken dürften sich etliche infizierte Rechner finden. Ein Alptraum für Administratoren, die mit dem Problem gerade in Form der Wundertüte "Notebook im Außeneinsatz" noch eine geraume Zeit zu kämpfen haben werden. In milderem Licht erscheint die Lage auch deshalb nicht, da sich das Ziel des unerwünschten Untermieters, nämlich die DNS-Einstellungen zu ändern, als äußerst simpel darstellt. Viele IT-Verantwortliche dürften sich da die Frage stellen, wie viele eventuell deutlich folgenreichere Schädlinge sonst noch ihr Unwesen treiben.

Doch der Security-Admin hat nicht nur mit offensichtlicher Schadsoftware zu kämpfen. In einem Beitrag ab Seite 62 erklären wir, wie sich das Kommunikationstool Skype durch proprietäre VoIP-Protokolle geschickt einer Kontrolle entzieht und die systematische Filterung seines Datenstroms nahezu unmöglich macht. Wer das Netzwerk einem Penetrationstest unterziehen will, sollte sich unseren Workshop ab Seite 42 ansehen. Dieser zeigt auf, wie Sie mit der Linux-Distribution BackTrack 5 Ihr System auf mögliche Schwachstellen prüfen. In einem Test ab Seite 16 muss mikado Macmon beweisen, wie gut es sich bei der Network Access Control schlägt. Außerdem haben wir für Sie ab Seite 36 in einem Einkaufsführer zusammengestellt, auf was KMUs bei der Gefahrenabwehr achten sollten.

Die Redaktion des IT-Administrator wünscht Ihnen ein frohes Weihnachtsfest und einen guten Rutsch ins neue Jahr.

Ihr

Lars Nitsch
Redakteur

System- und Plattformsicherheit

Im Test: Realtech theGuard! 7

Wichtige IT-Komponenten im Unternehmensnetzwerk müssen rund um die Uhr überwacht werden. Mit dem neuen theGuard! 7 fasst Realtech zahlreiche Funktionen zum Monitoring, Netzwerk-Management und Business Process Management zusammen. Dank "Root Cause Analysis" sollen Administratoren dabei Fehlern auf den Grund gehen können. Wie das funktioniert und welche Neuerungen Version 7 mitbringt, hat sich IT-Administrator für Sie angeschaut.

Seite 27

Penetrationstest mit BackTrack 5

Sicherheitsprodukte aus dem Open Source-Umfeld haben Hochkonjunktur – gerade solche, die im Vergleich zu kommerziellen Lösungen eine vergleichbare Funktionalität bieten. Ein Musterbeispiel hierfür ist die Linux-Distribution BackTrack, die der Durchführung von Penetrationstests und dem Sammeln sicherheitsrelevanter Informationen dient. Das Tool gilt als eine Art Schweizer Hacker-Taschenmesser, das auf das Aufspüren von Sicherheitslücken und den Security-Check einzelner Rechner in Netzwerken spezialisiert ist. Die Software vereint alle wichtigen Werkzeuge und erlaubt es, schnell und ohne großen Aufwand Sicherheitsanalysen durchzuführen. Unser Workshop zeigt die Konfiguration von BackTrack und den Einsatz der Scanner sowie der Schwachstellenwerkzeuge.

Seite 42

AKTUELL

PRODUKTE

PRAXIS

WISSEN

RUBRIKEN

Risiken beim Einsatz von Instant Messaging und Skype

Trotz der vielfach beschworenen Einheitlichkeit der Kommunikationsplattformen auf Basis von Unified Communications ist vielen Arbeitgebern der Frieden am Arbeitsplatz wichtiger als alle Sicherheitsbedenken. Aus diesem Grund werden in vielen Unternehmen auch weiterhin Anwendungen wie beispielsweise Skype und andere IM-Dienste nicht von den Client-Rechnern verbannt. Dieser Beitrag zeigt technische und rechtliche Risiken beim Einsatz von Instant Messaging-Produkten auf und untersucht diese Gefährdungen im Detail am Beispiel Skype.

Seite 62

Malware-Schutz beim Landessportbund Nordrhein-Westfalen

Ein oft unterschätztes Einfallstor für Malware sind mobile Devices wie Smartphones und Notebooks, die von Außendienstmitarbeitern genutzt werden. Zudem besitzen kleine und mittlere Unternehmen nicht selten nur eingeschränkte Ressourcen und Budgets für ihre IT-Sicherheit. Dies bedeutet, dass die Security-Software nicht immer auf dem neuesten Stand ist, da Wartungsaufgaben oftmals noch manuell durch den Administrator durchgeführt werden müssen und dadurch dringend benötigte Ressourcen, zum Beispiel für das Update von Virendatenbanken, blockiert sind. Einem ähnlichen Szenario sah sich bis Ende letzten Jahres auch die IT-Abteilung des Landessportbunds Nordrhein-Westfalen ausgesetzt.

Seite 74

Themenübersicht

Bestellen Sie jetzt das IT-Administrator Sonderheft II/2011!

180 Seiten Praxis-Know-how rund um das Thema

SharePoint 2010 für Administratoren

zum Abonnenten-Vorzugspreis von*

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft II/2011 für € 24,90. Nichtabonnenten zahlen € 29,90. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.*

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier
www.it-administrator.de/kiosk/sonderhefte/

Mehr Druck für Arbeitsgruppen

Xerox erweitert sein Portfolio an **Druckern und Multifunktionssystemen** um drei neue Modelle: die Multifunktionssysteme der **WorkCentre 5300-Serie, das Xerox WorkCentre 6015 sowie den Farbdrucker Xerox Phaser 6700**. Beim WorkCentre 6015 hat Xerox nach eigener Aussage Wert auf eine einfache Konfiguration und Bedienung gelegt. Die Druckgeschwindigkeit beträgt mit HiQ-LED-Drucktechnologie 12 Seiten pro Minute bei Farbausdrucken und 15 Seiten pro Minute in Schwarzweiß. Mit einer Druckgeschwindigkeit von bis zu 45 DIN-A4-Seiten in Farbe oder Schwarzweiß in einer Auflösung von 2.400 x 1.200 dpi richtet sich der Phaser 6700 dagegen an mittlere und große Arbeitsgruppen. Zu den Features zählt unter anderem die Bedienung über einen Farb-Touchscreen. Auf dem Bedienfeld kann der Anwender Videos aufrufen, die ihm beispielsweise zeigen, wie er Verbrauchsmaterial nachfüllt oder spezielle Funktionen aufruft. Für Ausdrucke im Format DIN-A3 sind die Schwarzweiß-Multifunktionssysteme der WorkCentre 5300-Serie ausgelegt. Die Modelle 5325, 5330 und 5335 spucken 25, 30 beziehungsweise 35 Seiten pro Minute aus. Alle drei neuen Systeme sollen sich durch einen besonders sparsamen Energieverbrauch auszeichnen.

Das Xerox WorkCentre 6015 soll sich durch seine leichte Bedienbarkeit auszeichnen

Die WorkCentre 6015-Serie beginnt bei 199 Euro, die Phaser 6700-Geräte sind ab 1.175 Euro erhältlich. Für die WorkCentre 5300-Serie hingegen werden mindestens 4.750 Euro fällig. *(dr)*

Xerox: www.xerox.de

Unified Storage für Einsteiger

NetApp baut sein Angebot an **Unified Storage-Systemen** aus und bringt mit dem Modell **FAS2240** eine neue Appliance auf den Markt, die sich primär an mittelständische Unternehmen richtet. Der Neuzugang erweitert die FAS2000-Serie, die bisher in der Variante 2040 auf zwei Höheneinheiten maximal 12 Festplatten zur Verfügung stellte. Das neue FAS2240 kommt in einer 2U- und einer 4U-Variante in den Handel und beherbergt höchstens 24 Laufwerke, die eine Brutto-Kapazität von bis zu 54 TByte bereitstellen. Maximal lässt sich das System mit Erweiterungseinheiten auf bis zu 144 Drives skalieren. Anschluss ans Netzwerk findet der Speicher über das Fibre Channel-Protokoll, iSCSI sowie CIFS und NFS. In der Basis-Version findet der Datenaustausch über GBit-Ethernet (maximal acht Schnittstellen) statt, mit optionalen Steckkarten ist zudem eine Anbindung über 10-GBit-Ethernet oder 8-GBit-Fibre Channel möglich. Ein doppelter Controller soll für Ausfallsicherheit sorgen. Im Betriebssystem "Data ONTAP" sind ab Werk Thin Provisioning und Deduplizierung enthalten. Über die Features Multipath I/O, Sync-Mirror, MultiStore und MetroCluster will der Hersteller zudem die Hochverfügbarkeit der Plattform gewährleisten. Extra lizenzieren muss der Nutzer Funktionen zum Mirroring und zur Applikationsintegration. Der Preise für die FAS2000-Familie beginnen bei 6.150 Euro. *(ln)*

NetApp: www.netapp.com/de/

In der 4U-Variante der Unified Storage-Appliance FAS2240 von NetApp finden bis zu 24 Festplatten Platz

Nachvollziehbare Verzeichnisverwaltung

ScriptLogic bietet den **Active Administrator** in **Version 6.0** an. Die neue Version soll IT-Administratoren dabei helfen, **Probleme im Verzeichnisdienst zu identifizieren, Health Check-Ups durchzuführen** sowie **zeitlich festgelegte Berichte zu erstellen**. Dies gilt für die besonders kritischen Bereiche innerhalb des Active Directory: Konfiguration und Replikation. Der Active Directory Assessment Report ermöglicht eine Prüfung der AD-Infrastruktur, um Administratoren einen Überblick über die Domain und damit verbundene Informationen zu verschaffen. Dadurch sollen sich potenzielle Änderungen oder problematische Bereiche rasch ausfindig machen lassen. Der Replication Analyzer, ein neuer interaktiver Bereich, erleichtert zudem Replication Health-Prüfungen sowie das Monitoring. Die Resultate enthalten zusätzliche Informationen, die in Detailansichten einsehbar sind und sowohl generelle Fehler bei der Replikation als auch Informationen zu DNS-Testresultaten umfassen sollen. Dank seiner neuen Active Directory Maintenance-Tools erleichtert Active Administrator 6.0 laut Anbieter zudem die Verwaltung und Instandhaltung von Active Directory-Usern und Rechnern. Mit Account Maintenance-Tools für User und Rechner können Administratoren inaktive Anwender und PCs in der Domänenumgebung scannen, identifizieren und löschen. Eine Erinnerungsfunktion zur Passwortänderung ermöglicht es dem Admin, benutzerangepasste Erinnerungs-E-Mails zur Passwortänderung zeitlich festzulegen und zu automatisieren. Zu den Erweiterungen des Produktes gehören ferner Auditing-, Alerting- und Notification-Tools. Active Administrator 6.0 ist ab sofort erhältlich und kostet 10,90 Euro pro Lizenz. *(dr)*

ScriptLogic: www.scriptlogic.com

Mit Active Administrator 6.0 stehen Administratoren zusätzliche Active Directory-Verwaltungstools zur Verfügung

Viel Band auf wenig Platz

Overland Storage fügt seinem Portfolio an **automatisierten Bandbibliotheken** mit der **NEO 600** und der **NEO 800** zwei neue Modelle mit **LTO-5-Unterstützung** hinzu. Die Variante NEO 600 stellt in sechs Magazinen insgesamt 72 Slots für Bandkassetten bereit und bietet auf sechs Höheneinheiten bis zu 216 TByte Backup- und Archivkapazität. Die mit acht Magazinen und 96 Band-Parkplätzen größere Version NEO 800 archiviert in komprimierter Form bis zu 244 TByte in einem 8U-Formfaktor. Die Bandbibliotheken lassen sich mit maximal vier respektive sechs Laufwerken ausstatten und verfügen über redundante Netzteile. Anschluss ans Netzwerk finden die Geräte über 6 GBit-SAS oder 8 GBit-Fibre Channel. Nutzer bedienen die Archivierungs-Appliance über ein Touchscreen an der Frontseite oder remote über ein Webinterface. Durch die Unterstützung der LTO-5-Bandlaufwerktechnologie mit LTFS-Funktionalität (Linear Tape File System) lassen sich Dateien laut Hersteller auf Bändern genau wie auf Festplatten mit Drag & Drop ablegen. Overland richtet sich mit den neuen Produkten an Unternehmen, für die bei Backup und Archivierung niedrige Gesamtbetriebskosten sowie ein geringer Stromverbrauch entscheidend sind. Der Einstiegspreis für die beiden neuen Geräte liegt bei rund 11.500 Euro. *(ln)*

Overland Storage: www.overlandstorage.com

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

Von **Alt-N** kommt mit **MDaemon Messaging Server BlackBerry Edition 12.5** die neueste Version des E-Mail- und Groupware-Servers. Die Software ermöglicht jetzt nicht nur den drahtlosen Zugang zu E-Mail, Kontakten oder dem Kalender mit Hilfe des vollständig integrierten BlackBerry Enterprise Servers, sondern bietet durch das optional erhältliche ActiveSync-Modul ebenfalls die Möglichkeit der E-Mail- und Datensynchronisation für iPhone, Android und Windows Mobile. Ferner hat der Hersteller das LookOut-Theme der mitgelieferten Web-Oberfläche WorldClient überarbeitet und neu gestaltet, so dass jetzt auch Tablets wie das iPad oder das Playbook unterstützt werden. Administratoren können in der neuesten Version außerdem auf HTML-Domain-Signaturen zurückgreifen. Schließlich hat Alt-N die Sicherheitsfunktionen noch einmal erweitert. MDaemon Messaging Server BlackBerry Edition 12.5 ist ab 275 Euro erhältlich. *(ln)*
www.altn.de/md_main.cfm

nlyte bringt mit der **nlyte Express Edition** eine Einstiegslösung für das Data Center Infrastructure Management auf den Markt. Die Software besteht aus den vier Hauptkomponenten Bulk Data Manager, Datacenter Module, Planner Module und dem Organizer. Damit erstellt der Administrator ein zentrales Verzeichnis, in dem Informationen über alle Systeme in einem Rechenzentrum zusammengefasst sind. Das Werkzeug analysiert zudem, welche Abhängigkeiten zwischen den einzelnen Komponenten bestehen. Außerdem ermittelt die DCIM-Software in Echtzeit den Status der Systeme und erlaubt es, unterschiedliche Szenarien durchzuspielen. Der IT-Fachmann kann beispielsweise prüfen, welche Auswirkungen es hat, wenn er Racks mit Servern oder Netzwerkgeräten in einem bestimmten Bereich des Rechenzentrums aufstellt. Die nlyte Express Edition ist ab 800 Euro monatlich verfügbar. *(ln)*
www.nlyte.com

TAROX stellt das Serversystem **Parx104i G4** mit einer Höheneinheit vor. Der Server verfügt über vier Festplatten-Einschübe und richtet sich an kleine und mittlere Unternehmen. An Speichermedien lassen sich kostengünstigere SATA-Platten oder performantere SAS-Festplatten nutzen. Zudem lässt sich die Serverplattform mit der Hochverfügbarkeitslösung Stratus Avance kombinieren und unterstützt so mehrere virtuelle Maschinen mit einem Arbeitsspeicher von bis zu 32 GByte. Ab sofort ist der Server auf dem Markt erhältlich. Der Preis beginnt bei 1.099 Euro. *(dr)*
www.tarox.de

Ab sofort bietet **Matrix42** mit seinem **Mobile Device Management (MDM)** Managementfunktionen für iPhone, iPod Touch und iPad mit dem neuen iOS 5 an. Nutzer haben so die Möglichkeit, ihre E-Mails direkt per S/MIME zu verschlüsseln. Auch ist laut Hersteller eine einfache Konfiguration der Proxy-Einstellungen und automatische Einwahl in Wi-Fi-Netzwerke möglich. Die Lösung von Matrix42 basiert auf der Technologie von AirWatch. Das Mobile Device Management für iOS 5 ist ab sofort verfügbar. Der Preis für 100 Lizenzen beträgt 4.850 Euro. *(dr)*
www.matrix42.de/mdm

Ordnung im Admin-Gehege

Mit neuen Features und Optimierungen bringt **Cyber-Ark** die **Version 7.0** seiner **Privileged Identity Management Suite (PIM)** auf den Markt. Die neue Version unterstützt nun die **automatische Verwaltung und Überwachung von privilegierten Administratoren-Accounts in virtuellen Umgebungen**. PIM besteht aus vier komplementären Lösungsmodulen. Im Mittelpunkt steht der Enterprise Password Vault für die automatische Verwaltung von privilegierten Administratoren-Accounts. Er bietet eine geschützte Verwahrung und regelmäßige, automatische Änderung von Passwörtern. Weiterer Bestandteil ist der Privileged Session Manager, mit dem privilegierte Zugänge nicht nur im Hinblick auf das "Wer", sondern auch auf das "Was" gesichert und überwacht werden können. Der Application Identity Manager soll die in Skripten oder Config-Files eingebetteten statischen Passwörter eliminieren, während der On-Demand Privileges Manager die On-Demand-Bereitstellung von privilegierten Berechtigungen ermöglicht – eine differenzierte Vergabe von Superuser-Privilegien. Zu den Neuerungen in Version 7 gehört ein automatisches Provisioning und Deprovisioning von privilegierten, Root und Shared Accounts in VMware-Umgebungen unter ESX/ESXi und vCenter. Außerdem bietet das Update die sichere Verwahrung von Nutzerkennungen und Berechtigungsnachweisen in einem digitalen Datentresor, dem Digital Vault, ebenso wie eine Unterstützung von Audit- und Compliance-Anforderungen durch ein umfassendes Log-Management mit der Aufzeichnung aller Aktivitäten. Der Preis für den Privileged Identity Manager 7.0 beläuft sich bei zehn Administratoren auf 10.000 Euro. *(dr)*

Cyber-Ark: www.cyber-ark.com

F-Secure 2012 mit Kostenschutz

F-Secure stellt seine **Internet Security 2012** vor. Die Verbesserungen im neuen Release beinhalten unter anderem die Funktion **DeepGuard 4** und das damit verbundene intelligente Beobachten von Anwendungen. Außerdem will der Hersteller sowohl das manuelle und **Echtzeit-Malware-Scanning** als auch das sichere Entfernen von Malware optimiert haben. Das Cloud-basierte Echtzeitschutz-Netzwerk von F-Secure liefert unmittelbar Reputationsdaten über Webseiten und Dateien. Ein ebenfalls neues Feature der F-Secure Internet Security 2012 ist der Schutz von Windows 7-Nutzern vor unerwünschten mobilen Breitbandverbindungen und den dadurch entstehenden hohen Kosten. Die Software optimiert automatisch die Nutzung mobiler Breitbandverbindungen, egal ob im heimischen Netzwerk oder im Ausland. So sollen unliebsame teure Überraschungen, die durch 3G-Verbindungen entstehen, von Anfang an verhindert werden. Zusätzlich bietet F-Secure die F-Secure Internet Security 2012 Plus an. Sie soll die Produkte Internet Security 2012 und Mobile Security verbinden und einen umfassenden Schutz für Rechner und Smartphone oder Tablet PC bieten. Eine Lizenz der Internet Security 2012 ist beispielsweise für rund 30 Euro zu haben. Ferner bietet F-Secure für Unternehmen Business-Bundles an. *(dr)*

F-Secure will in seiner 2012er-Version vor unerwünschten 3G-Verbindungen schützen

F-Secure: www.f-secure.de

Mit Speed in die Cloud

Citrix Systems erweitert die **NetScaler SDX-Plattform** um den **Citrix Branch Repeater** – einen **virtuellen Dienst zur Beschleunigung von Anwendungen und Desktops in Niederlassungen**. Damit wird laut Anbieter die Bereitstellung von Anwendungen und Services aus der Cloud oder dem zentralen Rechenzentrum für Mitarbeiter in Zweigniederlassungen weiter beschleunigt. Die Architektur von NetScaler SDX unterstützt außer Citrix-Services auch Netzwerkdienste von Drittanbietern. Kunden verfügen so über eine offene virtuelle Plattform zum Aufbau eines Cloud-fähigen Netzwerks. Neben der neu hinzugekommenen WAN-Optimierung bietet NetScaler SDX die Bereitstellung von Web-Anwendungen, Lastausgleich, Firewall-Funktionen sowie SSL-verschlüsselten VPN-Remotezugriff in nur einer Appliance. Die WAN-Optimierungsfunktionen beinhalten zudem verschiedene Weiterentwicklungen der Citrix HDX-Technologie und unterstützen jetzt Links mit einem Durchsatz von bis zu 1 GBit/s. Der Dienst Branch Repeater 1000 ist ab sofort auf dem NetScaler SDX 13505 verfügbar. Er unterstützt bis zu 1 GBit/s an XenDesktop- oder XenApp-Datenverkehr. Darüber hinaus optimiert die Lösung bis zu 6.000 HDX-Nutzer-Sessions gleichzeitig. Der Preis des Branch Repeater 1000 beginnt bei 265.000 US-Dollar. Ebenfalls ab sofort erhältlich ist der Branch Repeater 500, der auf dem NetScaler SDX 11505 läuft. Er unterstützt bis zu 500 MBit/s an XenDesktop- oder XenApp-Datenverkehr und optimiert bis zu 3.000 HDX-Nutzer-Sessions parallel. Der Preis dieser Variante beginnt bei 170.000 US-Dollar. Der Branch Repeater 500 lässt sich jederzeit mittels einer "Pay-As-You-Grow"-Lizenz auf die Kapazität des Branch Repeater 1000 erweitern. *(dr)*

Citrix: www.citrix.de

Gewinnen Sie eine Synology DS212+

Pünktlich zum Weihnachtsfest bietet Ihnen IT-Administrator die Gelegenheit, Ihren Gabentisch um ein **nagelneues NAS** zu bereichern und verlost eine **Synology DS212+**. Die Synology DS212+ wurde für kleine und mittlere Unternehmen entwickelt und liefert eine durchschnittliche Lesegeschwindigkeit von 109 MBit/s und eine Schreibgeschwindigkeit von 56 MBit/s in RAID 1-Konfigurationen. Mit USB 3.0-Unterstützung für Übertragungsgeschwindigkeiten von bis zu 5 GBit/s, 10 mal schneller als USB 2.0, benötigt die DS212+ weniger Zeit für die Datenübertragung auf externe Festplatten und verbraucht weniger Strom. Zusätzlich machen die HotSwap-Laufwerke die Wartung und den Austausch von Festplatten einfacher. Der Hersteller verspricht über die umfassende Netzwerkprotokoll-Unterstützung ein nahtloses Austauschen von Dateien über Windows-, Mac- und Linux-Plattformen. Die Windows ADS- und LDAP-Integration ermöglichen, das Gerät schnell und auf einfache Weise an eine bestehende Unternehmens-Netzwerkumgebung anzupassen, ohne Benutzerkonten neu erstellen zu müssen. Die Synology DS212+ läuft mit der System-Firmware "Synology DiskStation Manager" und bietet speziell für SMBs entwickelte Anwendungen und Funktionen. Das Directory Server Paket macht aus dem Synology DS212+ einen LDAP-basierten Verzeichnisserver, der sich für die Zentralisierung der Verwaltung und Authentifizierung von Benutzerkonten unterschiedlicher Applikationen eignet und so die Netzwerksicherheit verbessert. Um an der Verlosung teilzunehmen, senden Sie bis zum 09. Januar 2012 eine E-Mail mit dem Betreff "Synology" an redaktion@it-administrator.de und teilen uns darin mit, was die Synology DiskStations für den Unternehmenseinsatz noch attraktiver machen würde. *(jp)*

Mit etwas Glück bringt Ihnen der Weihnachtsmann eine Synology DS212+

Schnelles Backup von virtuellen Servern

Quantum vergrößert sein Portfolio zur **Datensicherung in virtuellen Umgebungen** um die **Appliance vmPRo 4601**. Das Modell fungiert als eine schlüsselfertige Backup-Lösung für virtuelle Maschinen in Infrastrukturen unter VMware und richtet sich vor allem an klein- und mittelständische Unternehmen sowie Zweigstellen. Die Backup-Anwendung schreibt Daten direkt auf eine integrale Ziel-Disk, nutzt dabei Deduplizierung für langfristige Datenvorhaltung und weist laut Hersteller schnelle Wiederherstellungsraten auf. Der Backup-Neuling mit Unterstützung für vSphere5 verfügt über eine eingebaute Kapazität, die sich in 4 TByte-Ausbaustufen bis zu 12 TByte mittels einfacher Aktivierung des Lizenzschlüssels aktivieren lässt. Laut Quantum reduziert die zwei Höheneinheiten messende Appliance im Rack-Gehäuse das Backup-Volumen um bis zu 75 Prozent und speichert die virtuellen Maschinen in ihrem nativen Format auf den Deduplizierungs-Systemen. Dadurch will der Hersteller einen mehrstufigen Recovery-Prozess vom proprietären Backup-Format vermeiden, um dem Nutzer zu beschleunigten Recovery-Zeiten zu verhelfen. Das Backup-Werkzeug ist zu einem Preis ab 17.350 Euro erhältlich. Größeren Unternehmen stellt Quantum vmPRo als reine Software zur Verfügung, die in Verbindung mit den DXi-Deduplizierungs-Appliances des Herstellers für ein effizientes Backup und Restore im Rechenzentrum sorgen soll. *(ln)*

Die Backup-Appliance für virtuelle Umgebungen vmPRo 4601 von Quantum verrichtet ihren Dienst im Gehäuse einer DXi4600 – klingt komisch, ist aber so

Quantum: www.quantum.com/de/

Flexible Datenhaltung

Quantum bringt zwei **neue Storage-Systeme** auf den Markt. Sie sollen kleineren Unternehmen **Datendeduplizierungs- und Disaster Recovery-Lösungen** zu einem erschwinglichen Preis bieten. Die NDX-8 NAS-Appliance verfügt über 8 TByte NAS-Speicher mit eingebauter Backup-Software sowie Deduplizierungs-Technologie und ermöglicht laut Hersteller eine Reduktion des Speicherbedarfs um bis zu 90 Prozent. Die Appliance wird dabei mit Quantum Datastor Shield vorkonfiguriert ausgeliefert, das agentenloses Client-Backup unterstützt und die Installation der Software auf den zu sichernden Klienten überflüssig macht. Da die NAS-Serie das Windows Storage Server-Betriebssystem nutzt, können Nutzer Windows-basierte Applikationen wie Microsoft Exchange direkt darauf installieren. Für einen Offsite Disaster Recovery-Schutz kann die NDX Daten auf eine zweite NDX-Appliance replizieren oder diese über eine RDX 8000 außerhalb des Standorts transferieren. Gleichzeitig bringt Quantum mit der RDX 8000 eine 8-Slot Disk-Library mit Wechselplatten-Cartridges und 8 TByte Kapazität auf den Markt. Das Modell ist mit allen verfügbaren RDX-Medien mit einer Speicherkapazität von 160 GByte bis zu einem 1 TByte kompatibel und ermöglicht damit, die Größe des Systems den Erfordernissen anzupassen. Für 2012 plant der Hersteller außerdem die Auslieferung eines 1,5 TByte RDX Medien-Cartridges, das die Maximal-Kapazität der RDX 8000 um bis zu 50 Prozent auf 12 TByte erweitert. Der Preis etwa für die Quantum NDX-8d Appliance mit Datendeduplizierung liegt bei 4.165 Euro (ohne Deduplizierung 3.265 Euro). Die RDX 8000 kostet 4.050 Euro mit Datendeduplizierung beziehungsweise 3.150 Euro ohne. Nutzer der NDX-Appliances können zwischen einer Tower- oder einer 1U-Rack-Konfiguration wählen. *(dr)*

Quantum: www.quantum.com/de

Citrix Synergy, 25. bis 28. Oktober, Barcelona

Von der PC- zur Cloud-Ära

von Christian Knermann

Vom 25. bis 28. Oktober 2011 lud Citrix Systems zur "Citrix Synergy Europe 2011" nach Barcelona. Besonders der Weg vom klassischen PC hin zur Cloud stand für das Unternehmen im Fokus. Nicht nur hierfür hat Citrix mittlerweile zahlreiche Anbieter geschluckt und so sein Produktportfolio verbreitert, wie in Barcelona deutlich wurde. IT-Administrator war für Sie vor Ort.

Nachdem die Synergy [1] im Jahr 2010 erstmals einen Ableger in Europa bekommen hatte, standen nun im spanischen Katalonien alle Zeichen auf Wachstum. Mit über 3.900 Teilnehmern aus aller Welt fand sich ein gegenüber dem Vorjahr deutlich größeres Publikum ein, um sich aus erster Hand über neue Produkte zu informieren. Der erste Veranstaltungstag bot genügend Zeit für die Anreise und begann erst am späteren Nachmittag. Im Rahmen der "Geek Speak Live"-Reihe von Podiumsdiskussionen tauschten sich Citrix-Mitarbeiter sowie unabhängige Analysten und Blogger über aktuelle Themen aus. Mit Teilnehmern wie Shawn Bass, Rick Dehlinger, Douglas Brown und Gabe Knuth waren durchaus bekannte Namen aus den Bereichen Virtualisierung und Cloud vertreten, die spannenden Informationsaustausch garantierten. Nach den Diskussionsrunden bot sich die Gelegenheit, die Ausstellungshalle zu besuchen, wo neben Citrix selbst viele Partnerunternehmen mit Ständen vertreten waren, um ihre Lösungen vorzustellen.

Terminalserver keineswegs altmodisch

Der zweite Tag begann mit einem ersten Block von 45-minütigen Breakout-Sessions. Ein überraschend großer Andrang herrschte bei der Sitzung zur neuesten Version 6.5 von XenApp. Die hohe Besucherzahl ließ darauf schließen, dass sich aller Euphorie über Desktop-Virtualisierung zum Trotz der klassische Terminalserver immer noch großer Beliebtheit erfreut. Der Vortrag stellte insbesondere sämtliche neuen Funktionen in den Vordergrund, die der weiteren Optimierung der Benutzerfreundlichkeit dienen. So etwa erlaubt der sogenannte "Session Pre-Launch", häufig benutzte Anwendungen im Hintergrund bereits zu starten, sobald ein Benutzer seine Anmeldeinformationen eingibt. Der Anwender kann so seine Anwendung deutlich schneller aufrufen. Wird die Anwendung anschließend beendet, hält das neue "Session Lingering" die Sitzung im Hintergrund für eine definierbare Zeitspanne aktiv, so dass beim nächsten Start der Anwendung nicht erneut ein kompletter Anmeldevorgang durchlaufen werden muss.

Weiterhin wurde demonstriert, dass das ICA-Protokoll mit der Erweiterung HDX erneut Verbesserungen erfahren hat, die die Übertragung von Multimedia-Daten, insbesondere Flash, über WAN-Verbindungen betreffen. Das "Citrix Service Provider Automation Pack", das bislang als separater Download Citrix-Partnern vorbehalten war, ist nun fester Bestandteil von XenApp. Den Kern bildet ein Satz von Gruppenrichtlinien und PowerShell-Scripts, die die Optik eines Windows Server 2008 R2 Desktops weitestgehend an Windows 7 angleichen sollen, um im Zusammenspiel von XenApp und XenDesktop ein einheitliches Erscheinungsbild zu gewährleisten.

Neues im Portfolio

Nach diesem ersten Block von Informationen stand die mit Spannung erwartete Keynote auf dem Programm, zu der sich die Teilnehmer in das Auditorium begaben. In diesem überdimensionalen Kinosaal fanden alle Besucher Platz und bekamen eine beeindruckende Show geboten. In über zwei Stunden stellte Citrix-CEO Mark Templeton mit Unterstützung einiger Spezialisten eine Unmenge an neuen Entwicklungen vor. Die Reihe begann mit der Integration von Kaviza in das Citrix-Produktportfolio. Citrix hatte den Anbieter einer Desktop-Virtualisierungs-

lösung für kleinere Unternehmen bereits vor einiger Zeit übernommen. Die erste Version von Kaviza unter der Flagge von Citrix heißt nun VDI-in-a-Box. Weiter ging es mit einem plakativen Hinweis auf das Jahr 2014 als Ablaufdatum für Windows XP. Als Antwort auf die vielerorts stockende Migration hin zu Windows 7 kündigte Mark Templeton die Übernahme des bisherigen Citrix-Partners App-DNA mit seinem Produkt AppTitude an. Es darf vermutet werden, dass diese Übernahme eine Reaktion auf die Übernahme des Herstellers ChangeBASE durch Citrix' Mitbewerber Quest darstellt. Das Produkt AppTitude ermöglicht – ganz ähnlich zu ChangeBASE AOK – in drei Schritten die automatisierte Analyse aller Applikationen eines Unternehmens im Hinblick auf die Kompatibilität zu Windows 7. Im zweiten Schritt können, soweit möglich, Inkompatibilitäten gefixt und im dritten Schritt zu für Windows 7 passenden MSI-Paketen geschnürt werden.

Vom PC zur Cloud

Als übergreifendes Thema kam Templeton daraufhin auf die Entwicklung von der endenden PC-Ära hin zur Cloud-Ära mit den drei Säulen Personal, Private und Public Clouds zu sprechen. Im Folgenden stellte er, begleitet von einigen Live-Demos, Citrix' Angebote für diese drei Bereiche vor. So adressiert Citrix die Personal Cloud, in deren Mittelpunkt die Daten der Anwender stehen, mit der bereits im Vorfeld bekannt gewordenen Übernahme von ShareFile. Der Dienst erlaubt es Anwendern, mit einem Outlook-Plug-in auf einfache Weise auch größere Datenmengen per E-Mail zu versenden, indem die Daten in die Cloud hochgeladen werden und statt der eigentlichen Datei nur ein Link übermittelt wird. Ein Synchronisations-Tool ermöglicht es weiterhin, Daten über mehrere Rechner und mobile Geräte konsistent zu halten. Das Online-Tool GoToMeeting wird zudem um eine Funktion namens "Workspaces" ergänzt, die das gemeinsame Online-Arbeiten an Dokumenten mit sich bringt. Als drittes Standbein soll laut Templeton auch der Citrix Receiver selbst das Synchronisieren von Daten lernen. Eine entsprechende Tech-Preview soll noch bis Ende 2011 erscheinen. Mit all diesen Funktionen will Citrix das Prinzip "Follow-Me Data" etablieren, das Anwendern ihre Daten überall und auf all ihren Endgeräten auf sichere Weise zugänglich macht.

Im Rahmen der Private Cloud geht es darum, Anwendungen zusammenzufassen und an die Anwender zu liefern. Zu diesem Zweck stellte Templeton das neue Citrix CloudGateway mit den sogenannten Storefront Services vor. Dieses Gateway bietet den Anwendern sämtliche für sie freigegebenen Applikationen und Desktops nach Art eines App Stores an, aus dem sie ihre Arbeitsumgebung individuell zusammenstellen können. In der kostenlosen Express-Variante wird das CloudGateway das bisherige Citrix-Webinterface ersetzen und nur XenApp- sowie XenDesktop-Sitzungen transportieren. Die Enterprise-Variante soll zusätzlich auch den Zugriff auf beliebige Web-Anwendungen, weitere SaaS-Angebote und Daten erlauben. Entsprechende APIs werden es Drittanbietern ermöglichen, die Funktionalität zu erweitern. Auf Seiten des Rechenzentrums soll die kürzlich erfolgte Übernahme von RingCube helfen, die persönlichen Daten und Einstellungen der User in einer separaten virtuellen Disk vom Master Image eines Remote Desktops zu entkoppeln und so die Verwaltung zu vereinfachen.

Client-seitig soll zukünftig die Implementierung von HDX in einem Hardware-Chip die Verarbeitung des Remote-Protokolls beschleunigen. Zur Entwicklung eines entsprechenden System-on-Chip (SoC) verkündete Templeton die Kooperation von Citrix mit ncomputing und Texas Instruments. Erste Endgeräte als Ergebnis dieser Zusammenarbeit sollen 2012 erscheinen. Als dritten Baustein führte Templeton die Public Cloud an und erläuterte, wie sich die Produkte der ebenfalls übernommenen cloud.com ins Portfolio einfügen sollen. Zu einer neuen Version der IaaS-Plattform CloudStack gesellt sich CloudPortal als Managementlösung, mit der Service Provider auf einfache Weise Cloud-basierte Dienste an ihre Kunden bringen können. Wer sein lokales Rechenzentrum in die Cloud ausdehnen möchte, kann dafür das Produkt CloudBridge nutzen, das in Verbindung mit dem Citrix NetScaler nach Bedarf die Brücke zwischen lokalen IT-Diensten und Ressourcen von Cloud-Anbietern schlägt.

Die Besucher hatten anschließend die Möglichkeit, die Themen der Keynote in zahlreichen weiteren Breakout-Sessions zu vertiefen. Am nächsten Morgen startete die Agenda um neun Uhr mit zusätzlichen Sessions und den Learning Labs. Dabei handelte es sich um dreistündige Sitzungen für bis zu 32 Personen, in denen ausgewählte Inhalte aus Citrix Schulungen vorgestellt wurden, die die Teilnehmer in einer Demo-Umgebung direkt selbst ausprobieren konnten. Die Labs waren zwar bereits im Vorfeld der Veranstaltung ausgebucht, da dennoch viele reservierte Plätze frei blieben, bot sich für Frühaufsteher aber vor Ort die Chance, von der Warteliste nachzurücken. Aufgrund der großen Resonanz auf die Labs hatte Citrix die Agenda zudem bis auf den Freitag ausgedehnt und weitere Kurse dieser Art angeboten.

Fazit

Die Synergy war definitiv einen Besuch wert. Die Konferenz bot eine unglaubliche Vielfalt an Informationen, zum einen im Hinblick auf konkrete technische Informationen zu Kernprodukten wie XenApp oder XenDesktop. Zum anderen war allerdings die Bandbreite an Ankündigungen [2] von neuen Produkten und Lösungen in Bezug auf strategische Überlegungen zum Cloud Computing fast erschlagend und vermittelte den Eindruck, dass Citrix hier derzeit zahlreiche Eisen im Feuer hat. Zu vielen der neuen Entwicklungen wurde noch kein Verfügbarkeitsdatum genannt und so bleibt es spannend zu beobachten, ob und wie sich alle Mosaiksteine im Laufe der kommenden Monate zu einem stimmigen Gesamtbild zusammenfügen werden. Bis dahin bleibt als Ausblick, dass die Synergy auch im nächsten Jahr wieder in Barcelona stattfinden wird. *(dr)*

[1] Citrix Synergy Barcelona
BBA21

[2] Citrix Synergy-Newsroom
BBA22

Link-Codes

SNW Europe, 2. und 3. November, Frankfurt/M.

Bewölkt mit Niederschlag

von Lars Nitsch

Unter dem Leitspruch "Powering the Cloud" stand die Europa-Ausgabe der diesjährigen Storage Networking World ganz im Zeichen der Wolke. Dass von einem bewölkten Himmel nicht selten Niederschlag fällt, erfuhr die Speicher-Branche schmerzhaft und ganz direkt. So ist durch die Überflutungen in Thailand und die damit verbundenen Produktionsausfälle in den nächsten Monaten mit einem erheblichen Preisanstieg bei Festplatten zu rechnen. Doch IT-Administrator stieß in Frankfurt auch auf gute Neuigkeiten – nach Deduplizierung und Data Tiering wird besonders das Thema Desaster Recovery für den Mittelstand preislich immer attraktiver.

Die Gerüchteküche auf der SNW bestätigte die Befürchtungen: Festplattenhersteller gehen aufgrund der Überflutungen in Thailand von einem Preisanstieg von bis zu 150 Prozent aus – Tendenz steigend. In Anbetracht dieser Hiobsbotschaft haben einige Storage-Hersteller noch einmal die Lager gefüllt. So orderten gerade kleinere Hardware-Anbieter in den Tagen vor den Preissprüngen noch zusätzliche Chargen an Magnetspeichern. Erst ab Mitte kommenden Jahres ist wieder von einer Erholung der HDD-Preise auszugehen.

Besucherzahlen auf Vorjahresniveau

Rund 1.850 Teilnehmer diskutierten auf der diesjährigen SNW aktuelle Themen und Trends aus der Storage-Welt, fast 200 mehr als noch im Vorjahr. Abzüglich der 500 Sponsoren-Vertreter fällt der Anstieg jedoch nicht mehr ganz so beeindruckend aus – alles in allem blieb das Fachbesucher-Niveau ungefähr erhalten. Diese Stagnation spiegelt sich auch anhand der Zahl der Aussteller wider, die in diesem Jahr genau 70 Messestände errichtet haben – zwei weniger als zwölf Monate zuvor. Symantec etwa war gar nicht mit einem eigenen Stand vertreten, andere namhafte Hersteller setzten eher auf einen kleineren Auftritt. Von NetApp war zu vernehmen, dass das Unternehmen jedes Jahr seine Messe-Aktivitäten überprüfe und die SNW 2012 noch keineswegs gesetzt sei.

40.000 US-Dollar pro PByte

Beeindruckend war wie immer die Zahl der Vorträge – über 130 Dozenten vertieften sich in teilweise praxisnahe, manchmal aber auch theoretische Ausführungen, die im Großen und Ganzen den Themenbereichen Storage-Technologien und -Virtualisierung sowie Cloud Computing zugeordnet waren. So erfuhren die Zuhörer beispielsweise, dass bei der Speicher-Virtualisierung unterschiedliche Queue-Tiefen beim Einsatz von Tiered Storage nicht selten zu Problemen führen. VMware stellt mit "Adaptive Queue Depth Algorithm" zwar schon länger ein Gegenmittel zur Verfügung, dies ist jedoch vom Administrator manuell zu aktivieren – eine Tatsache, derer sich kein einziger Admin im durchaus üppig gefüllten Auditorium bewusst war.

Das (Problem-)Bewusstsein schärfte zudem so manche Zahl – so gehen Experten davon aus, dass 1 PByte Speicherplatz derzeit mit 40.000 US-Dollar zu Buche schlägt und bis 2015 rund 80 Prozent aller File-Daten auf virtualisierten Servern liegen werden. Auch die stetig steigende Kapazität von Festplatten – bis 2015 sollen 10 TByte durchaus in Reichweite sein – sorgt für Schwierigkeiten. Insbesondere die Mean Time Between Failures steigt bei immer mehr Plattern und höherer Sektorendichte bis in den unpraktikablen Bereich an.

Desaster Recovery goes Mainstream

Doch der Admin lebt im Hier und Jetzt, und so konnten sich gerade die Storage-Verantwortlichen von kleinen und mittleren Betrieben über gute Nachrichten freuen. Beim Thema Desaster Recovery deutet sich ähnlich zur Deduplizierung ein Spill-Over-Effekt vom Enterprise-Bereich in den KMU-Sektor an. Mehrere Anbieter haben mittlerweile Appliances im Angebot, die das Thema Datenschutz und -wiederherstellung im Katastrophenfall mit durchaus erschwinglichen Appliances oder eigenen Software-Lösungen adressieren.

Ein weiterer Dauerbrenner ist das Backup von virtuellen Servern. Laut einer Untersuchung des Data Protection-Anbieters Bocada nutzt eine große Mehrheit der Systemverantwortlichen zwei verschiedene Backup-Lösungen für die Sicherung virtueller und physikalischer Server. Dass dies nicht gerade für ein Plus an Übersichtlichkeit sorgt und die Verwaltbarkeit virtualisierter Infrastrukturen erschwert, liegt auf der Hand. Erschwerend kommt hinzu, dass neben dem bekannten Wildwuchs bei virtuellen Maschinen auch bei den so einfach anzufertigen Snapshots eine rasante Zunahme erfolgt. Ein nicht zu vernachlässigendes Storage-Problem, wenn hunderte oder gar tausende von Snapshots Speicherplatz belegen.

Fazit

Alles in allem lässt sich zur SNW 2011 wieder einmal das Fazit "Der Mix macht's" ziehen. Erfreulich fiel auf, dass das Ausmaß an "Consumerization" im Storage-Sektor noch nicht allzu ausgeprägt ist und das gut informierte Fachpublikum die Chance zum Ideenaustausch am Schopf packt. Auch 2012 wird sich dazu wieder Gelegenheit bieten – die SNW findet dann am 30. und 31. Oktober statt.

STRATO

Der perfekte Auftritt macht unseren Erfolg: auf dem Laufsteg und im Web.

Stefan Klos

Stefan Klos
www.famepr.de
Erstellt mit dem PowerPlus-Paket

Hosting

Für Anwender mit hohen Ansprüchen

Ihre Website mit echten Profi-Features

- ✓ Bis zu 12 Domains und 10.000 MB Speicher
- ✓ Unlimited Traffic und 20 MySQL-Datenbanken
- ✓ Profi-Features: PHP, Perl, Python und Ruby 8
- ✓ **NEU!** Contao – Content Management System für Profis

Power Hosting

schon ab **0,–** €/Mon.* für 3 Monate

AKTION BIS 31.12.2011!

Erfolgreicher durch einzigartige Website-Gestaltung

12designer	content.de EINFACH GUTER INHALT	SNACK TV
Persönliche Website-Designs	Individuelle Texte	Professionelle Videos

Jetzt bestellen unter: **strato.de/hosting**

Servicetelefon: 0 18 05 - 055 055
(0,14 €/Min. aus dem dt. Festnetz, Mobilfunk max. 0,42 €/Min.)

* Alle PowerPlus-Pakete 3 Monate 0 €/mtl., danach PowerPlus 6,90 € mtl., PowerPlus L 14,90 €/mtl. und PowerPlus XL 24,90 €/mtl. Einrichtungsgebühr 14,90 €. Mindestvertragslaufzeit 6 Monate. Preise inkl. MwSt.

The Quest Experts Conference Europe, 17. bis 19. Oktober 2011, Frankfurt/M.

Think Big

von John Pardey

Quest rief zur "Experts Conference" (TEC) und alle Experten machten sich auf den Weg nach Frankfurt, um den für die zum zweiten Mal in Folge in Deutschland stattfindende Veranstaltung ausgerufenen Anspruch der "Level 400"-Vorträge Realität werden zu lassen. Die von Microsoft stammende Einordnung der technischen Tiefe von Trainings und Präsentationen definiert Level 400 als "Expert material. Assumes a deep level of technical knowledge and experience…". Und genau das bekamen rund 350 Teilnehmer an drei Tagen in Sachen Active Directory, Exchange, Virtualisierung und PowerShell in rund 100 Vortragsslots geboten.

Den Kern der Experts Conference bildet nach wie vor eine umfangreiche Vortragsreihe rund um Verzeichnisdienste aus dem Hause Microsoft – maßgeblich das Active Directory, aber auch ADFS oder FIM. Dabei standen den Teilnehmern allein in dieser Vortragsreihe teilweise bis zu drei Präsentationen gleichzeitig zur Auswahl.

Dabei boten sich den IT-Verantwortlichen einerseits die klassischen technischen Themen, wie zum Beispiel der Vortrag von Ulf B. Simon-Weidner, Consultant für Microsoft-Plattformen bei der Computacenter AG und Autor des IT-Administrator Sonderhefts "Active Directory", zum Thema IPv6 und Active Directory. Seine im Vortragstitel formulierte Frage "Do I dare or am I scared?" (Soll ich's wagen oder zögern?) ließ sich nach seinen Ausführungen mit einem "Dare" beantworten, auch wenn er aus seiner Praxis von einigen unschönen Phänomenen beim IPv6-Einsatz zu berichten wusste.

Andererseits wird das Active Directory im Zeitalter der Cloud immer mehr zum Träger einer weit über die Unternehmensgrenzen hinausreichenden "Identity". Dieses Thema veranschaulichten die Experten in zahlreichen Beispielen, etwa bei der Zusammenarbeit mit SharePoint 2010 über Organisationsgrenzen oder auch dem Einsatz der Microsoft Cloud-Dienste Azure und Office 365.

Nicht ohne mein Exchange

Wird über das Active Directory diskutiert, ist natürlich auch der Exchange Server nur einen Steinwurf entfernt. Und so war es nur logisch, dass die TEC auch dieses Jahr wieder zahlreiche Slots zur Messaging-Plattform im Angebot hatte. Und selbstverständlich wurde auch hier das absolute Expertenniveau gehalten, wenn es um Themen wie die Migration von Exchange 2007, Hochverfügbarkeit oder Troubleshooting ging.

Eine Ansammlung von Experten wie in den Exchange-Tracks findet sich sonst vermutlich nur auf Microsofts TechEd. Aus Redmond selbst kamen Ilse Van Criekinge, Greg Taylor und Ross Smith – alle Mitglieder der Exchange- und Unified Communications-Produktteams bei Microsoft und so natürlich mit Informationen aus erster Hand bestens versorgt. Aber auch der unseren Lesern aus den diesjährigen Exchange-Trainings bekannte Jürgen Haßlauer und der Leiter der deutschen Exchange User Group, Walter Steinsdorfer, waren als Dozenten vor Ort.

Cloud statt SharePoint

Stand im vergangenen Jahr noch SharePoint 2010 im Fokus der TEC, entschieden sich die Organisatoren bei Quest dieses Jahr, eine Vortragsreihe zu Virtualisierung und Cloud aufzusetzen. Dabei stand naturgemäß Microsofts Hypervisor Hyper-V im Mittelpunkt der Präsentationen, etwa der von Guido Grillenmeier, Chief Engineer der Enterprise Services Group bei HP, der von seinen Erfahrungen aus einem Virtualisierungsprojekt mit mehr als 1.000 Servern berichtete. Diese wurden zunächst mit der Version 1 von Hyper-V von ihrem physikalischen Dasein in ein virtuelles überführt, um sie im weiteren Verlauf des Projekts auf Hyper-V Version 2 zu migrieren. Zur Überraschung vieler Zuhörer konnte er dabei nur von sehr wenigen Schwierigkeiten berichten.

Ebenfalls auf sehr viel Anklang stieß die Vorstellung des neuen Virtual Machine Managers 2012 aus der Microsoft System Center-Reihe. Dieses Werkzeug, das mittlerweile Hosts mit allen wichtigen Hypervisoren verwalten kann, hat das Potential, den Nutzen der Virtualisierung etwa durch Automatisierung und Self Service auf eine neue Stufe zu heben.

Fazit

Zum zweiten Mal in Folge ließ Quest die TEC in Deutschland verweilen. Und doch bestand die Teilnehmerschaft aus einem sehr internationalen Feld – deren Urteil nach die TEC auf jeden Fall eine Reise wert ist. Und vom Niveau der Vorträge ist sie dies definitiv. Als Wermutstropfen bleibt lediglich anzumerken, dass sich ein Großteil der Präsentationen an wirklich große Unternehmen und Organisationen richtet. Wer jedoch als Admin in einem solchen Umfeld tätig ist, sollte definitiv die Augen offenhalten für den nächsten Termin der Experten in Europa.

Netezza. Läuft schon nach 24 Stunden.

IBM Netezza Data Warehouse läuft innerhalb von 24 Stunden und rechnet sich ebenso schnell. Denn IBM Netezza Data Warehouse ist so leistungsstark, dass es anspruchsvolle Analysen in kürzester Zeit erstellt. So können Sie Ihr Unternehmen nicht nur schneller machen, sondern auch Ihre Ergebnisse beschleunigen.

ibm.com/netezza/de

IBM, das IBM Logo, ibm.com und das Bildzeichen des Planeten sind Marken oder eingetragene Marken der International Business Machines Corporation in den Vereinigten Staaten und/oder anderen Ländern. Andere Namen von Firmen, Produkten und Dienstleistungen können Marken oder eingetragene Marken ihrer jeweiligen Inhaber sein. Eine aktuelle Liste der IBM Warenzeichen finden Sie im Internet unter www.ibm.com/legal/copytrade.shtml. © 2011 IBM Corporation. Alle Rechte vorbehalten.

Im Test: mikado Macmon NAC 3.3

Wirkungsvolle Einlasskontrolle

von Thomas Bär

In den allermeisten Unternehmen gibt es nach wie vor eine Unterscheidung zwischen innen und außen. Hat es ein IP-fähiges Gerät erst einmal in das interne Netzwerk geschafft, steht der Zugang zu zahlreichen Ressourcen offen. Network Access Control ist eine Technologie, um diesen Zugang zu kontrollieren und bei Bedarf einzuschränken. Gemeinhin gilt das Verfahren als komplex und schwierig zu administrieren. Die Software Macmon von mikado macht deutlich, dass dem nicht so sein muss.

Das Anschließen eines Computers an ein lokales Netzwerk, sei es per Kabel oder per WLAN, ist heute selbst für den unbedarften Benutzer keine Herausforderung mehr. In der Regel beschränkt sich dieser Schritt auf das "Anstecken" – möglicherweise noch einen WLAN-Schlüssel eintippen – fertig. Die Einfachheit ist in vielen Umgebungen absolut wünschenswert, da sie die Anzahl von Einsätzen durch den IT-Support gering hält. Unpraktisch indes, sofern eine wie auch immer gewollte oder entstandene Richtlinie im Unternehmen das Verbinden von unbekannten Maschinen untersagt oder ausgewählte Netzwerkbereiche selektiv aus der Situation heraus bereitgestellt werden sollen.

Windows Server-Bordmittel mit 802.1x erfüllen NAC unzureichend

Das Mittel der Wahl für den Administrator stellt in diesem Fall die Network Access Control (NAC) dar. Mit dem Erscheinen von Windows Server 2008 wurde erstmalig ein Netzwerkzugriffsschutz direkt in den Basisumfang eines Windows-Betriebssystems integriert. Dieser Netzwerkzugriffsschutz, im Englischen von Microsoft als "Network Access Protection" (NAP) bezeichnet, bietet Administratoren eine Möglichkeit, die Sicherheit im Unternehmensnetzwerk zu verbessern. Wie bei NAC so verschiebt auch Windows in erster Linie Computer, die nicht den Sicherheitsanforderungen entsprechen, in ein "Zwischennetzwerk", um diese auf den gewünschten Sicherheits- oder Patch-Stand zu bringen. Erwartungsgemäß arbeitet NAP von Microsoft lediglich mit Windows und zwar in der Version XP SP3 und höher. Ältere Systeme oder Nicht-Windows-Computer wie Smartphones, IP-Telefone oder Apple iPads bleiben komplett unberücksichtigt.

Microsoft baut dabei auf zwei Techniken auf: DHCP und IEEE 802.1X. In der einfachsten Implementierung prüft Microsoft-NAP bei Vergabe einer IP-Lease den Status des Client-Systems und modifiziert in Abhängigkeit vom Ergebnis die zu vergebende IP-Adresse. Dieses System lässt sich zwar sehr einfach durch den Administrator aufbauen, verliert jedoch seine Schutzfunktion, sobald einem Rechner eine feste IP-Adresse zugewiesen wird. In der weitaus sichereren Variante prüft Windows Server mittels 802.1X-Standard und eines RADIUS-Servers die durch den Teilnehmer (Supplikant) übermittelten Authentifizierungsinformationen und regelt den Zugriff auf die durch den Authenticator angebotenen Dienste wie LAN, VLAN oder WLAN. Da keine eigenen Authentisierungsprotokolle definiert wurden, empfiehlt der Standard das Extensible Authentication Protocol (EAP) oder das PPP-EAP-TLS Authentication Protocol. Nachteilig bei Verwendung von 802.1X ist jedoch, dass die entsprechende Infrastruktur zunächst mühselig aufgebaut werden muss und zudem ein ordentliches Know-how der Thematik vom Administrator verlangt wird.

Skalierbares Macmon

Die Besonderheit von Macmon, aktuell in der Version 3.3 verfügbar, ist die Möglichkeit, das System in wachsenden Ausbaustufen zu betreiben. So kann der Administrator die Netzwerksicherheit Schritt für Schritt erhöhen, ohne sich von Anfang an mit einer sehr großen und komplexen Infrastruktur abgeben zu müssen. Das Kernsystem Macmon bietet die Fähigkeit, MAC-Adressen gezielt in VLANs zu lenken, den Netzwerkzugriff zu erlauben oder zu unterbinden und die MAC-Adressen nach verschiedenen Verfahren

Systemvoraussetzungen

64 Bit-Hypervisor-Virtualisierungsumgebung wie VMware ESX und 2 GByte Arbeitsspeicher, mindestens 30 GByte Platz für virtuelle Festplatten und eine aktuelle 64 Bit-CPU.

zu ermitteln. In größeren Ausbaustufen wird das 802.1X-Verfahren für über WLAN angebundene Endgeräte genutzt, werden Gastnetzwerke implementiert und ein IF-MAP-Server mit Statusinformationen versorgt beziehungsweise abgerufene Statusinformationen verarbeitet.

Die Entwickler bei mikado setzten dabei auf allgemein anerkannte Techniken wie das Simple Network Management Protocol (SNMP), Informationen aus dem DHCP-Server, ARP-Analysen oder ausgewertete Netbios-Namen von Client-Rechnern. Die konsequente Verwendung von Standard-Protokollen erlaubt einen möglichst herstellerunabhängigen Einsatz der Software.

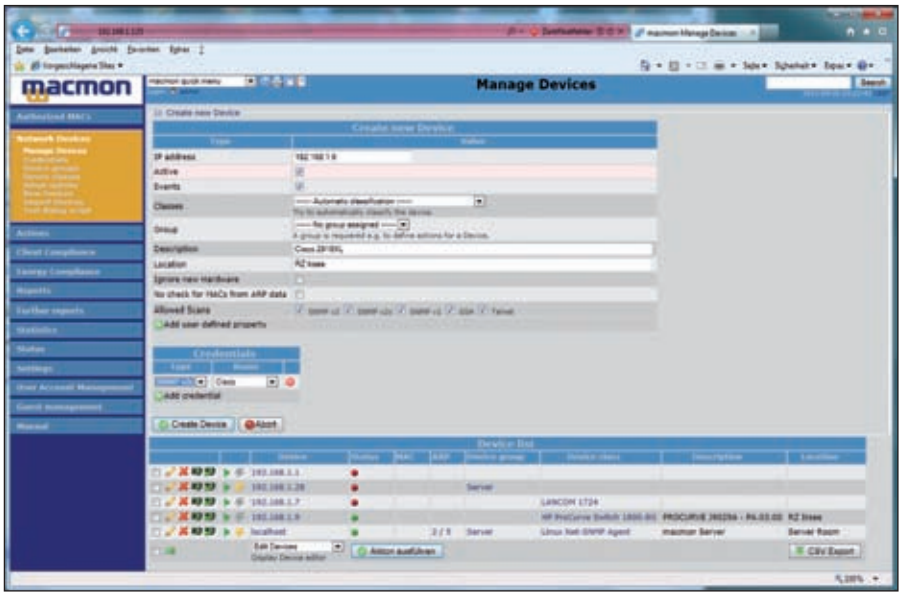


Bild 2: Die Anlage der Aktivkomponenten wie Switches, Router oder Server ist einer der ersten Schritte unter Macmon. Die automatische Geräte-Erkennung umfasst jedoch nur einen Teil der am Markt verfügbaren Geräte.

Installation der virtuellen Appliance

mikado liefert Macmon als zentrale Software für eine ganze Reihe von Erweiterungen, die so genannten "Options", sowohl als physikalische als auch virtuelle Appliance aus. Wir entschieden uns im Test für eine 60-Tage-Version der virtuellen Appliance, die im Open Virtualization Format (OVF)-Format ausgeliefert wird. Der Download der knapp 850 MByte großen Appliance zog sich über das Internet ein wenig hin, da die Performance des Downloads nicht unbedingt die beste war. Die Lizenzdatei erhielten wir per E-Mail innerhalb weniger Stunden durch den Hersteller.

Zunächst versuchten wir ergebnislos, die OVF-Datei mit der Virtual Appliance unter VMware Workstation 7 zum Laufen zu bringen. Obwohl OVF als allgemeiner und offener Standard von virtuellen Maschinen durch die Distributed Management Task Force (DMTF) definiert wurde, scheint es immer wieder Probleme beim Import der Pakete zu geben. An sich ist OVF nicht auf eine bestimmte Hypervisor- oder Prozessor-Architektur beschränkt und eignet sich so hervorragend für die Bereitstellung von virtuellen Appliances. Eingespielt unter VMware ESX 4.0i war die Macmon-Appliance binnen zwei Minuten einsatzfähig.

Bild 1: Die Grundeinstellungsoberfläche von mikado Macmon sieht der Administrator eher selten. Automatische Backup-Funktionen, die Integration in eine SNMP-gestützte Netzwerküberwachung und eine deutschsprachige Oberfläche überzeugen.

Die Appliance, ausgestattet mit zwei zugewiesenen CPUs, 2 GByte RAM, drei Netzwerkkarten und einer virtuellen 30 GByte Festplatte, basiert auf Debian Linux 5.0 und beinhaltet alle benötigten Komponenten wie eine MySQL-Datenbank oder einen Webserver. Eine der drei Netzwerkkarten zieht sich per DHCP eine IP-Lease und unter dieser Adresse ist die Konfiguration über das Webinterface sofort möglich. In den Grundeinstellungen ist über Webmin lediglich die Sprache einzustellen und das Update auf die aktuellste Version durchzuführen. Die Zugangspasswörter findet der Benutzer im beiliegenden PDF-Dokument bei der OVF-Datei. Das Update – wieder knapp 150 MByte – wurde eingespielt. Ein Vorgang, der einige Minuten Zeit in Anspruch nahm, dann konnte die Software genutzt werden.

Die Konfiguration nimmt der Administrator über eine verschlüsselte HTTPS-Verbindung zum Webserver vor. Eine unsichere HTTP-Verbindung bietet Macmon erst überhaupt nicht an: Eine Grundeinstellung, bei der sich viele andere Softwareanbieter sehr gern ein Beispiel nehmen können. Nach der Eingabe der Lizenzschlüssel schauten wir zunächst etwas verwundert auf das Webinterface, da die rote Meldung mit dem Hinweis auf eine fehlende Lizenz nicht verschwinden mochte. Eine E-Mail an den Support

united-domains.de präsentiert:

Die neuen Domains kommen!

Das Rennen um die besten Namen hat begonnen.

Jetzt kostenlos vorbestellen

Die Internet-Verwaltung ICANN hat das „new gTLD Programm“ freigegeben.
Neben den bekannten Domain-Endungen, wie .de oder .com, wird es ab 2012 zahlreiche **„neue“ Domain-Endungen, wie .web, .shop, .film, .berlin** oder **.bayern** geben.

united-domains bietet Ihnen schon jetzt die Möglichkeit, sich beim Rennen um die besten Namen einen guten Platz zu verschaffen.

Jetzt Ihre Wunsch-Domains kostenlos vorbestellen unter:
www.united-domains.de

united domains

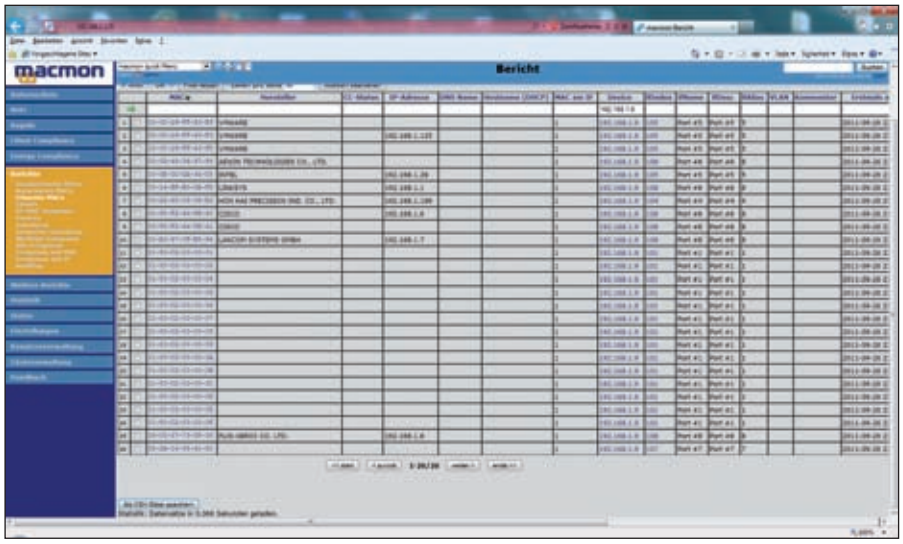


Bild 3: Bereits nach kurzer Zeit liefert mikado Macmon die ersten Übersichten an protokollierten MAC-Adressen. Die Daten stammen aus den überwachten Switchen.

konnte dies auch zu späterer Stunde klären: Es wurde versehentlich keine Appliance-Lizenz übermittelt – am morgigen Tag würde Abhilfe geschaffen –, was auch zeitnah geschah.

Start ohne Installationsassistent

Bewaffnet mit der richtigen Lizenz konnte der Test der Software nun beginnen – einige Switches verschiedener Hersteller, ein Microsoft Windows Server 2003 Domänen-Controller mit aktiviertem SNMP-Dienst, etwas WLAN-Infrastruktur und einige Client-Computer warteten auf die Zuordnung durch mikado Macmon. Die zu lösende Aufgabe: einem ausrangiertem Windows XP Rechner den Zutritt zum Netzwerk verweigern – unabhängig davon, an welcher Netzwerkdose das Gerät angeschlossen wird. Diese Konstellation ist der kleine Bruder der Einstellung, alle unbekannten MAC-Adressen grundsätzlich auszusperren.

Wer in der Weboberfläche der Software eine automatische Suchfunktion im Stil "IP-Bereich {von} {bis}" erwartet, dessen Suche wird vergebens sein. Aktive Netzwerkinfrastruktur-Geräte wie Switche oder Router muss der Administrator dem System manuell bekanntmachen. Hierzu wird im insgesamt sehr übersichtlichen Webinterface auf Englisch oder Deutsch in der linken Menüstruktur "Devices" gewählt. Für die Eingabe ist lediglich die IP-Adresse notwendig – die automatische Hardware-Erkennung konnte die Testgeräte von Hewlett Packard, Cisco, Dell und LANCOM sicher identifizieren. Unmanaged Switches und Geräte für den Hausgebrauch bieten üblicherweise nicht die geforderten Fähigkeiten des VLANs. Uplinks zwischen den Switches identifiziert Macmon automatisch, verlangt jedoch vom Anwender eine einmalige Zuordnung.

Etwas ärgerlich für den Nutzer ist das Fehlen eines Installations-Assistenten. Nachdem der erste Switch angelegt war, erschien der Dialog zur Eingabe der SNMP-, Telnet- und SSH-Zugangsdaten. Diese wurden aber noch nicht definiert. Somit war erst einmal die Konfiguration der Zugangsinformationen für die drei Versionen von SNMP, Telnet und SSH angesagt. Glücklicherweise lassen sich die Zugangsdaten an "Gerätegruppen", beispielsweise Routern oder Switches, anhängen – somit gilt die dort definierte Zugriffsart.

Dokumentiert und ausgesperrt

Über die Software lassen sich problemlos die Ports auf den Switches ein- und ausschalten oder als "trusted" definieren. Hierzu muss der Administrator Macmon nicht verlassen und auf die herstellerspezifischen Interfaces wechseln. Überhaupt gefiel uns die Aufschlüsselung der gesammelten Informationen in Tabellenübersichten. Wechselt ein Gerät den Anschluss und taucht an einem anderen Port wieder auf, so wird dies protokolliert. Wann wurde die MAC-Adresse erstmals gesehen, wann zuletzt und wo und unter welcher IP-Adresse – alles wird dokumentiert.

Alle gesammelten MAC-Adressen von den verschiedenen Geräten werden über ARP oder das proprietäre Cisco-Protokoll CDP ermittelt und in der Datenbank abgelegt. In der Grundeinstellung sammelt Macmon nur diese Informationen, sperrt diese Geräte jedoch nicht aus. Über CSV-Imports könnten die MAC-Adressen auch manuell eingelesen werden. Für den

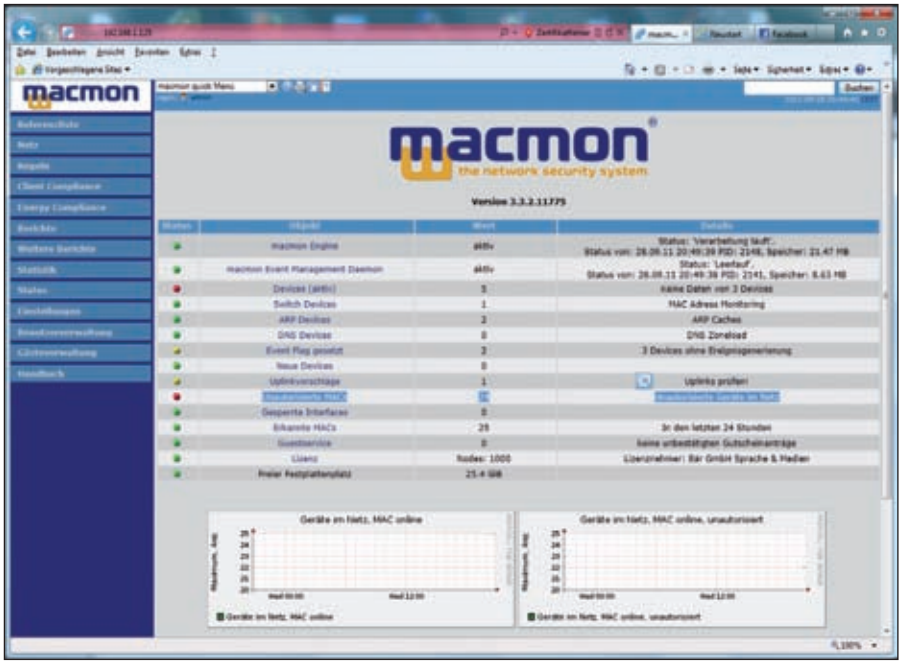


Bild 4: Im Übersichtsfenster von mikado Macmon wird der Administrator gleich auf die Anzahl nicht autorisierter MAC-Geräte aufmerksam. In einer auf Sicherheit getrimmten Umgebung wird unbekannten MAC-Adressen der Zugriff verweigert.

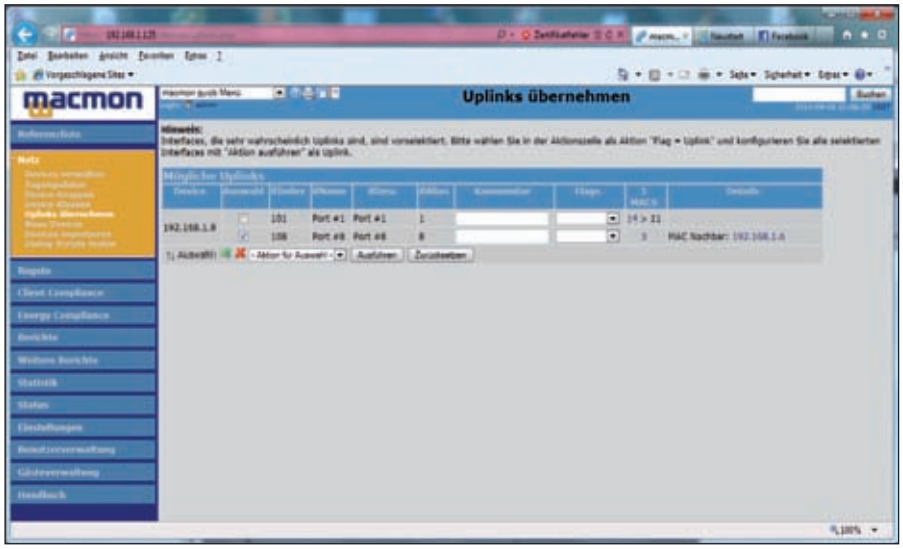


Bild 5: Uplinks zwischen den Switchen und Routern erkennt die Software automatisch – der Administrator muss lediglich die fixe Verbindung der Aktivkomponenten bestätigen

bereits benannten Windows XP-Rechner wurde festgelegt, dass dieser in ein spezifisches VLAN verschoben wird, sobald er an einem Port auftaucht. Das funktionierte im Test – sofern der Switch in der Lage war, VLANs zu steuern. Der HP ProCurve 1800-G machte uns hier einen Strich durch die Rechnung – schreibende Aktionen über SNMP unterstützt das Gerät nicht.

Blick über den Tellerrand

Wir betrachteten im Test nur die erste Sicherheitsstufe von Macmon 3.3. Im Vergleich zur Microsoft-Variante bietet sie den Vorteil, dass sie losgelöst von der Geräteart arbeitet. Telefone, Tablet-PCs, Thin Clients, Drucker oder Zeiterfassungsterminals profitieren besonders von diesem Verfahren, da sie mit IEEE 802.1X in den seltensten Fällen zusammenarbeiten. 802.1X als Sicherungsverfahren unterstützt mikado Macmon dennoch, da laut Hersteller nur über diese Authentifizierung ein gesichertes WLAN aufgebaut werden kann. Eine leider ausschließlich für Windows-PCs verfügbare Software von mikado erlaubt im Zusammenspiel mit Macmon auch die Prüfung der Security-Compliance. Diese überwacht den Patch-Stand des Clients, ist in der Lage, den TPM (Trusted Plattform Module)-Chip abzufragen oder prüft, ob der Benutzer Administrationsrechte besitzt.

Ergänzend im System von Macmon hat der Hersteller weitere Optionen im Lieferumfang: Die Funktion "Advanced Security" prüft beispielsweise, ob sich die Gestalt einer MAC-Adresse verändert hat. Somit werden gespoofte MAC-Adressen identifiziert und vom Netzwerkverkehr ausgesperrt. War eine MAC-Adresse monatelang stets ein Drucker und hat nun die Charakteristika eines Linux-Rechners, so greift der Schutz und vereitelt den Netzwerkkontakt. Die Option "Energy" überwacht die Energie-Einstellungen von Windows-Computern und prüft, ob diese möglicherweise sinnlos die ganze Nacht hindurch eingeschaltet sind. Energy wechselt zeitgesteuert das Energieprofil oder weckt die Computer rechtzeitig vor dem Eintreffen des Benutzers auf – als Individuallösung auch im Zusammenspiel mit dem Zeiterfassungssystem für Mitarbeiter oder Bewegungsmeldern.

Eine weitere Spielart von Macmon ist die Integration von anderen Sicherheitssystemen über "Active Incident Response" (AIR). Ermittelt beispielsweise ein Virenscanner von Kaspersky einen Virenbefall auf einer Workstation, so ist der zentrale Kaspersky-Server über eine Skript-Agent-Verbindung in der Lage, die IP-Adresse an Macmon zu übergeben. Dieser verschiebt auf dieses Signal hin die betreffende Maschine in ein dafür vorgesehenes VLAN.

Fazit

mikado Macmon ist eine insgesamt ausgereifte und auf Sicherheit getrimmte Software, deren weites Einsatzgebiet sich dem Administrator erst nach einiger Zeit überhaupt offenbart. Die automatische Erkennungsfunktion berücksichtigt bereits eine nennenswerte Anzahl von Geräten, ist aber bei Weitem nicht ausreichend für den Praxisbetrieb. Sofern die Methode der Scan-Aktionen jedoch einmal verstanden ist, verlieren unterschiedliche Aktivkomponenten ihren Schrecken – insbesondere, wenn die SNMP MIB-Files zur Verfügung stehen und deren Inhalt sich dem Administrator offenbart. Im Test konnte mikado Macmon durchaus überzeugen und die sicherlich langfristige Roadmap der Software verspricht noch einige spannende Erweiterungen. *(dr)*

Produkt
Software zur Network Access Control für größere Umgebungen und hohe Sicherheitsanforderungen.

Hersteller
mikado soft
www.mikado-soft.de

Preis
In der kleinsten Variante im Network-Bundle, bestehend aus Macmon NAC, Macmon Advanced Security und Macmon VLAN Manager, bei bis zu 250 Nodes 6.025 Euro inklusive einem Jahr Wartung.

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

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

Systemanforderung	7
Einrichtung und Bedienung	8
MAC-Schutzfunktionen	9
Integrierte Hilfen	5
Suchfunktion	5

Dieses Produkt eignet sich

optimal für Unternehmen, die eine sehr große Anzahl von aktiven Netzwerkkomponenten besitzen und sehr hohe Sicherheitsanforderungen stellen.

bedingt für relativ überschaubare Unternehmen, die ihre Betriebssicherheit erhöhen möchten.

nicht für kleine Unternehmen ohne aktive Netzwerkkomponenten.

mikado Macmon NAC 3.3 Network Security Bundle

Im Test: The Dot Net Factory AD Self-Service Suite 3.6

Selbstbedienung im Passwort-Laden

von Jürgen Heyer

Das Active Directory eignet sich sehr gut dazu, neben der Authentifizierung auch die Funktion einer zentralen Benutzerdatenbank mit Adressen, Telefonnummern und weiteren Attributen zu übernehmen. Mangels geeigneter Oberfläche können die Anwender auf diese Inhalte allerdings nur umständlich zugreifen. Dies ändert sich mit der AD Self-Service Suite, die das Active Directory in eine Informationsquelle für Benutzer umwandelt. Zusätzlich entlastet das Tool die Hotline, indem Anwender vergessene Passwörter selbst zurücksetzen können. Wir haben getestet, wie gut sich die Attribute und Kennwörter im Active Directory mit dem Werkzeug verwalten lassen.

Im Microsoft Active Directory (AD) wird es immer wichtiger, die zusätzlichen Attribute zu den Objekten, allen voran die Benutzerinformationen wie Abteilungszugehörigkeiten, Telefonnummern und Adressen, zu füllen, da viele Programme auf diese Inhalte zugreifen. Obwohl sich das AD in vielen Unternehmen somit immer mehr zu einer mächtigen Datenbank entwickelt, gibt es bei Windows kein richtiges Bordmittel, das es einem normalen Benutzer ermöglicht, auch direkt auf diese Daten zuzugreifen. Dies gelingt vielmehr nur über Umwege, wenn er beispielsweise in Verbindung mit MS Exchange über seinen Outlook-Client das Adressbuch nutzt, das wiederum den Inhalt aus dem AD bezieht.

Suite mit drei Modulen

Die 2005 gegründete Firma "The Dot Net Factory" hat sich im Microsoft-Umfeld auf Produkte für ein Identitätsmanagement sowohl für das Active Directory als auch für Multi-Plattformumgebungen mit LDAP-Verzeichnisdiensten spezialisiert. Die getestete AD Self-Service Suite (ADSS) ist dabei ein Einstiegsprodukt für Unternehmen, die die Möglichkeiten des AD zur Verwaltung der Benutzer sowie der dort gepflegten Geräte umfassender nutzen wollen. Die Suite beinhaltet dazu drei Module:

- Das Modul "AD WhitePages" liest das AD aus und präsentiert die Informationen durchsuchbar.
- Die zweite Komponente "AD Info" geht noch einen Schritt weiter und ermöglicht es einem Anwender, die eigenen im AD hinterlegten Informationen nicht nur einzusehen, sondern auch zu ändern beziehungsweise zu ergänzen.
- Das dritte Modul "AD Password" erlaubt es Anwendern, ihr Anmeldepasswort in Verbindung mit der Beantwortung einiger Sicherheitsfragen neu zu setzen, wenn sie es vergessen oder den Account durch zu viele Falscheingaben gesperrt haben.

Start mit einer hakelnden Installation

Die gesamte Suite ist nur rund 40 MByte groß, eine kompakte Installationsanleitung dazu ist verfügbar. Die darin enthaltenen Angaben zu den Installationsvoraussetzungen wie ein IIS-Server mit .NET-Framework und ASP.NET erwiesen sich aber nicht als vollständig, so dass es uns nicht auf Anhieb gelang, die Umgebung passend vorzubereiten. Wir nutzten zum Test zwei Windows-2008-Server, einen als Domänencontroller und einen als Webserver für den AD Self-Service in einem Netzwerk mit mehreren Clients. Da das eigentliche Setup keine Prüfung der Voraussetzungen durchführt, lief dieser Prozess auf Anhieb durch, sämtliche anschließenden Konfigurationsversuche führten jedoch zu ellenlangen, nur für einen Spezialisten interpretierbaren Fehlermeldungen. Erst ein Fernzugriff durch den Support des Herstellers mit einem anschließenden Hinweis, welche Features des IIS genau benötigt werden, lieferte die Lösung und schlussendlich eine lauffähige Einrichtung.

Bei der weiteren Konfiguration ist genau auf die Hinweise zu den Rechten der verwendeten Accounts zu achten, sonst sind Fehlermeldungen garantiert. Dies betrifft sowohl den Benutzer, der zur Konfiguration verwendet wird, als auch einen Account für Zugriffe auf das Dateisystem sowie die Er-

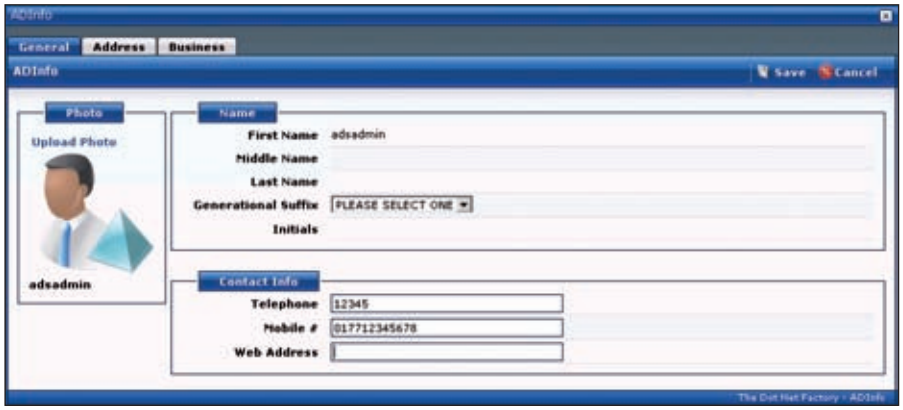


Bild 1: AD Info zeigt die eigenen AD-Informationen an und ermöglicht das Befüllen oder Ändern der freigegebenen Felder

eignisanzeige des Servers. Vorteilhaft ist, dass es für Letzteren eine Testfunktion gibt, ob die Rechte passen. Der Zugriff auf die einzelnen Funktionen der Suite geschieht je Modul über getrennte Webseiten, die anschließend angelegt werden. Diese lassen sich auf Wunsch in bereits vorhandene Sites integrieren, wobei wir für den Test die mit dem Webserver angelegte Standard-Site nutzten. Zu Redundanzzwecken sowie zur Lastverteilung kann die Suite auf mehreren Webservern installiert werden. Sofern ein SharePoint-Server genutzt wird, ist auch hier eine Integration möglich.

Insgesamt empfanden wir die Installation als etwas unrund, da die Voraussetzungen ungenau angegeben waren, diese weiterhin durch das Setup nicht geprüft wurden und zudem die ausgegebenen Fehlermeldungen keinen Rückschluss auf die eigentliche Ursache erlaubten.

Systemvoraussetzungen

Server-seitig wird aktuelle Hardware oder eine virtuelle Maschine mit 1 GByte RAM und 200 MByte Festplattenkapazität vorausgesetzt. Dazu Microsoft Windows Server 2003 oder höher, Microsoft IIS 6.0 oder höher, .NET Framework 2.0 mit ASP.NET sowie die Mitgliedschaft in einer Domäne.

Optional: Microsoft Windows SharePoint Services 2003, SharePoint Portal Server 2003, SharePoint 2007/2010.

Auf dem Client wird Microsoft Internet Explorer 7.0 oder höher oder Firefox 1.5 oder höher (Administration nur mit Internet Explorer) benötigt. Für den AD Password Client: Microsoft Windows XP SP1 oder höher, Vista 32/64 Bit, Windows 7 32/64 Bit, Microsoft Internet Explorer 7.0 oder höher.

Webbasierte Benutzeroberfläche mit Grafikproblemen

Nach Abschluss der Grundkonfiguration erfolgten alle weiteren Schritte über eine Webbasierte Administrationskonsole, ebenso wie die späteren Zugriffe der Anwender auf die einzelnen Module. Spätestens jetzt ist die vom Hersteller erhaltene Lizenzdatei manuell in ein vorgegebenes Verzeichnis zu kopieren. Dann sind die einzelnen Module in Verbindung mit den genutzten Domänen zu lizenzieren. Zu beachten ist hier, dass die Lizenzierung anhand der Anzahl der Benutzer-Accounts erfolgt, wobei es die Möglichkeit gibt, statt der gesamten Domäne gruppenweise zu selektieren. Weiterhin kann der Administrator an dieser Stelle sowohl die Administrationsrechte als auch die Rechte zum Aufruf der Module auf bestimmte Benutzer und/oder Gruppen einschränken. Hinsichtlich der Administration lassen sich ebenfalls einzelne Benutzer/Gruppen individuell auf die unterschiedlichen Funktionen berechtigen.

Anschließend muss der Administrator nochmals die verschiedenen ADs oder auch LDAP-Verbindungen eintragen, auf die die Suite zugreifen soll. Letzteres beschränkt sich aktuell auf ADAM, eine Unterstützung weiterer LDAP-Verzeichnisdienste ist in Entwicklung. Für jede Verbindung ist als Proxy-Account ein administrationsberechtigter Benutzer mit Passwort anzugeben. Alle Zugriffe auf die Verzeichnisdienste werden über diese Proxy-Benutzer abgewickelt.

Für einen ersten Test von Vorteil ist, dass die Suite mit vorbereiteten Standardansichten für die Module "AD WhitePages" und "AD Info" kommt. Dadurch sind nach Abarbeitung der bisher beschriebenen Konfigurationsschritte die ersten Aufrufe der Modulansichten möglich. Hilfreich ist dabei, dass rechts oben in der Administrationskonsole entsprechende Schaltflächen zu finden sind, die ein neues Browserfenster mit der entsprechenden Modulansicht öffnen. Das hat den Vorteil, dass sich Änderungen am Layout sofort kontrollieren lassen.

Für die Erstellung eigener Ansichten bietet die Suite einen Baukasten mit einzelnen Elementen wie Register, Gruppierungen und Attributen an. Die Attributsfelder enthalten dabei die eigentlichen Daten aus dem AD, die anderen Elemente dienen nur der Strukturierung. Hier wählt der Administrator die entsprechenden Elemente aus, wobei er nach Belieben gruppieren und die Reihenfolge der Felder festlegen kann. Über den Feldtyp lässt sich zudem steuern, ob ein Benutzer den Inhalt ändern kann oder nicht. Das ist insofern sinnvoll, weil ein Anwender fest vorgegebene Inhalte wie die Abteilung in der Regel nicht ändern können soll, er aber beispielsweise seine private Telefonnummer für die Kollegen hinterlegen kann. Bei den editierbaren Feldtypen gibt es Freitextfelder, in die der Benutzer beliebig schreiben kann, sowie Drop-Down-Listen, bei denen der Anwender aus einer vorgegebenen Liste auszuwählen hat.

Die grafische Aufbereitung übernimmt die Suite, hier gibt es keine weiteren Gestaltungsmöglichkeiten. Zu beachten ist auch, dass alle Feldbezeichnungen in Englisch sind. Für die Register und Gruppierungen darf der Administrator durchaus deutsche Begriffe verwenden, die englischen Labelbezeichnungen dagegen stammen aus dem AD, und hier kann er nur aus einer Liste wählen.

Die prinzipielle Vorgehensweise innerhalb der Module AD WhitePages und AD Info ist übrigens weitgehend identisch, dennoch gibt es einen Unterschied hinsichtlich der Zielsetzung: Während die AD WhitePages einen Blick auf das gesamte AD beziehungsweise einen gefilterten Bereich wie eine OU ermöglichen, bei Bedarf auch im Editiermodus, ist AD Info als Self-Service für einen Benutzer ge-

dacht, damit dieser seine eigenen Informationen einsehen und ändern kann. Nichtsdestotrotz lässt sich auch mit AD Info eine Ansicht bauen, um jedes Attribut aus dem AD anzeigen zu können.

Um einem Administrator gerade am Anfang die Arbeit zu erleichtern, hat er neben der Option, komplett neue Ansichten zu generieren, auch die Möglichkeit, eine vorhandene Ansicht zu kopieren und dann zu modifizieren. Wer AD WhitePages intensiv nutzen möchte, kommt aber um eine intensive Einarbeitung nicht herum. Dabei geht es weniger um die Bedienung der Administrationskonsole, sondern mehr um das Wissen, welche AD-Attribute überhaupt zur Verfügung stehen. So gibt es in der Konsole einen Auswahlpunkt "Directory Attributes", der die Attribute nach Objekttypen geordnet auflistet (unter anderem Benutzer, Gruppe, Computer, Drucker und Volume). Von den insgesamt 21 Objekttypen sind standardmäßig die zehn wichtigsten zur Ansicht ausgewählt. Pro Objekttyp stehen zwischen 9 und 201 Attribute zur Verfügung. Der Umfang ist also beachtlich.

Beim Arbeiten mit der Administrationskonsole in unserer Testumgebung zeigte sich ein deutlicher Optimierungsbedarf hinsichtlich des Umgangs mit den Fenstergrößen. So passen sich die Fenstergrößen leider nicht dynamisch an, wenn das Browserfenster vergrößert oder verkleinert wird. Beim Vergrößern bleiben rechts und unten weiße Streifen, beim Verkleinern wird die Ansicht einfach beschnitten, ohne dass Scrollbalken sichtbar werden. Vielmehr muss der Administrator erst die gesamte Ansicht aktualisieren lassen, damit alle Fenster an die aktuelle Größe des Browserfensters angepasst werden. Ärgerlich ist zudem, dass sich die Fenster oft in der Größe gar nicht verändern lassen wie beispielsweise bei der Attributauflistung. Hier werden pro Seite fest acht Attribute gelistet. Beim Objekt "Computer" mit 201 Objekten resultiert das in 26 Seiten, was die Handhabung umständlich macht. Beim Ergänzen von Attributen in den Ansichten von AD Info und AD WhitePages legen sich die kaskadierten Auswahlfenster so unglücklich übereinander, dass eine korrekte Auswahl kaum möglich ist. Auch registrierten wir gelegentlich Abstürze des Browsers beim Arbeiten in der Administrationskonsole vor allem beim schnellen Wechsel zwischen Punkten in der Menüleiste. Die Ansicht wurde dann zwar wiederhergestellt, nicht gespeicherte Änderungen gingen aber verloren.

Übersichtliches Infosystem für Anwender

Ein Benutzer wird mit den beschriebenen Problemen übrigens nicht konfrontiert, sie beschränken sich auf die Administrationskonsole. So passt sich in der Anwenderansicht bei den AD WhitePages die Fenstergröße auch dynamisch an das Browserfenster an. Das Modul überzeugt insgesamt als übersichtliches Informationssystem, mit dem sich gezielt nach Objekten suchen lässt. Die Möglichkeiten hängen natürlich sehr stark davon ab, welche Ansichten der Administrator zur Verfügung gestellt hat. Unterstützt wird ein Export nach Excel oder in eine HTML-Seite. Auch kann der Anwender aus den AD WhitePages direkt nach AD Info springen, sein Passwort ändern oder die unten noch genauer beschriebene Prozedur durchspielen, um später ein vergessenes Passwort selbst neu setzen zu können.

In den vorbereiteten Ansichten von AD WhitePages haben wir zwei praxisnahe Beispiele gefunden, die zeigen, wie leicht sich das Modul mit externen Funktionen verlinken lässt. So ließ sich hier nach Auswahl eines Benutzers über ein Register Google starten, um dort anhand des Anzeigenamens des Benutzers zu suchen. War weiterhin bei einem Account eine Adresse hinterlegt, so erschien in dessen Spalte ein kleines Hausobjekt. Bei einem Klick darauf wurde Google Maps gestartet und die Adresse auf der Karte angezeigt.

Flexibles Passwort-Recovery

Das Modul AD Password kann einen Benutzer-Account wieder freischalten, wenn dieser gesperrt ist, und gibt einem Anwender die Möglichkeit, sich ein neues Passwort zu vergeben, wenn er das alte vergessen hat. Dies funktioniert so, dass sich ein Benutzer vorher einmal über AD Password für diesen Prozess registrieren muss. Dabei muss er individuelle Antworten auf eine bestimmte Anzahl an Fragen geben, die gespeichert werden. AD Password kennt dazu drei Fragetypen: fest durch den Administrator vorgegebene Fragen, Fragen aus einer Auswahlliste sowie vom Benutzer selbst ausgedachte. Der Administrator gibt vor, wie viele dieser Fragen zu hinterlegen sind, und auch, wie viele für eine Entsperrung korrekt zu beantworten sind. Die Fragen und Antworten werden verschlüsselt im AD im normalerweise nicht verwendeten groupPriority-Attribut gespeichert.

Hat ein Benutzer nun sein Passwort vergessen oder muss er seinen Zugang nach zu vielen Falscheingaben entsperren, kann er in der Anmeldemaske seines PCs über eine zusätzliche Option in das Passwort Recovery Center springen und bekommt dort die Fragen gestellt. Hat er diese im gefor-

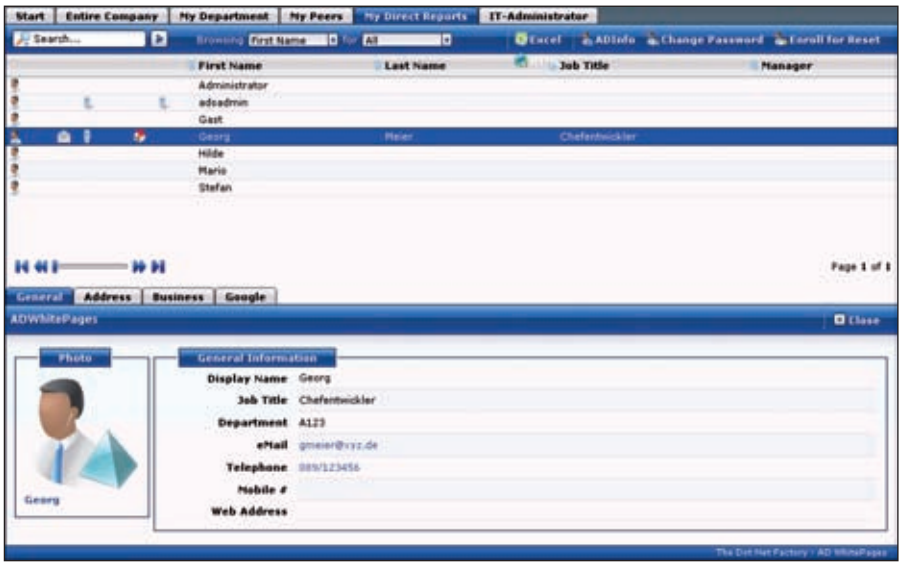


Bild 2: Mit AD WhitePages lässt sich über verschiedene Ansichten das AD durchsuchen. Der Administrator gibt dabei vor, was sichtbar sein soll.

STRATO PRO

Täglich eine Weihnachtsaktion!

Telefon: 0 18 05 - 00 76 77
(0,14 €/Min. aus dem dt. Festnetz, Mobilfunk max. 0,42 €/Min.)

strato-pro.de

* Beispielaktion am 01.12.11. PowerServer LX Managed: Keine Einrichtungsgebühr. Mindestvertragslaufzeit 12 Monate. Bei Überschreiten des Inklusiv-Transfervolumens 0,14 € je weiteres GB. Preise inkl. MwSt.

STRATO PRO

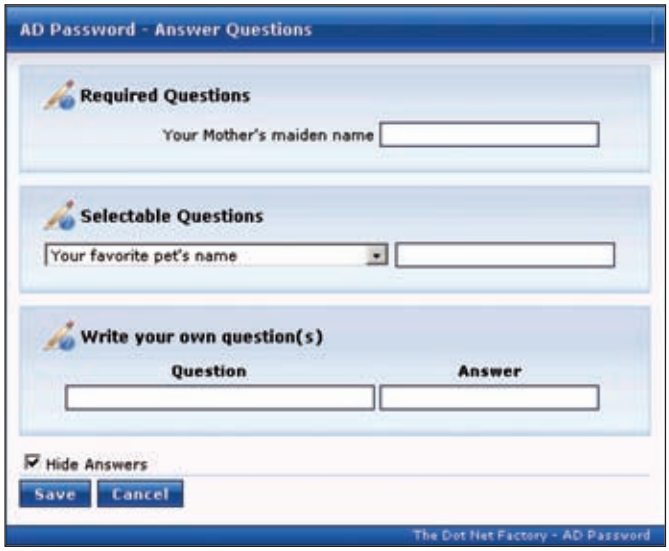


Bild 3: Über eine derartige Maske legt der Anwender bei der Registrierung die für ihn gültigen Sicherheitsfragen fest

dertem Umfang korrekt beantwortet, wird der Account entsperrt und er kann sein Passwort ändern. Damit die Anmeldemaske am Client diese zusätzliche Option anzeigt, ist die GINA (Windows Authentisierungsmodul) auszutauschen. Passende GINAs sind für Windows XP sowie Vista/7 (32 und 64 Bit) verfügbar. Zu beachten ist, dass kein anderes Programm installiert sein darf, das auch eine modifizierte GINA nutzt, sonst kommt es zu einem Konflikt.

Im Gegensatz zu den beiden anderen Modulen ist AD Password mit einer individuellen Sprachanpassung versehen. Pro Sprache wird ein eigenes Registerblatt mit zehn Unterregistern angelegt, wo für alle möglichen Meldungen die jeweiligen Texte einzutragen sind. Mit der Installation wurden im Test auch Reiter für Englisch, Französisch und Spanisch angelegt, es waren aber überall englische Texte eingetragen. Eine deutschsprachige Anpassung ist demnach selbst durchzuführen. Sie umfasst übrigens eine Vielzahl an Texten, da das Modul neben den eigenen Inhalten auch alle Meldungen seitens Windows zu den Passwortregeln wie Ablaufdatum, Länge und Passworthistorie sowie eventuelle Meldungen bei fehlerhaften Eingaben (Passworte sind nicht gleich, entsprechen nicht den Komplexitätsanforderungen und so weiter) umsetzen muss.

Individuell anpassbar sind weiterhin E-Mailbenachrichtigungen in Verbindung mit Passwortaktionen (unter anderem Zurücksetzen, Ändern, Entsperren und fehlgeschlagene Aktionen), wobei das Modul wahlweise den Benutzer selbst, den Administrator oder beide benachrichtigt. Das ist wichtig, um gegebenenfalls Eindringversuche zeitnah aufzudecken. Neben den Passwort-Regeln von Windows kann der Administrator auch für AD Password selbst festlegen, wie lange eine Registrierung gültig ist, also in welchen Abständen der Benutzer neue Fragen und Antworten wählen muss.

Funktional hat uns dieses Modul recht gut gefallen, auch wenn der Hersteller alle Sprachanpassungen auf den Kunden abwälzt. Ein derartiges Passwortmanagement durch den Anwender ist letztendlich immer eine Gratwanderung hinsichtlich der Sicherheit, wobei unserer Meinung nach bei AD Password ausreichend Möglichkeiten gegeben sind, über die Anzahl der zu beantwortenden Fragen die Hürde beliebig hoch zu setzen.

Fazit

Die aus drei Modulen bestehende AD Self-Service Suite 3.6 hat im Test einen durchwachsenen Eindruck hinterlassen. Am besten gefallen hat uns das Modul AD Password. Es beinhaltet eine komplette Sprachanpassung und lässt sich über eine frei festzulegende Anzahl an Fragen individuell an die jeweiligen Sicherheitsanforderungen anpassen. Zu beachten ist, dass an den Clients die GINA ausgetauscht werden muss, was zu einem Konflikt mit anderen Programmen führen kann, falls diese ebenfalls eine modifizierte GINA nutzen. Erfreulich ist die intuitive Anwendung, so dass die meisten Anwender ohne aufwändige Einweisung damit zurechtkommen sollten.

Die beiden Module AD WhitePages und AD Info sind aus Anwendersicht ebenfalls intuitiv bedienbar, wir vermissten im Test allerdings die Möglichkeit einer Sprachanpassung. Die Bedienung der Administrationskonsole bedarf aus unserer Sicht hier noch einer Optimierung. Wer die beiden Module über die bereits vorbereiteten Views der Benutzerdaten hinaus intensiv nutzen möchte, sollte eine umfassende Einarbeitung einplanen. Dies hängt weniger mit der Komplexität der Suite zusammen, sondern vielmehr mit der Vielzahl der im AD hinterlegten Attribute. *(jp)*

Produkt
Suite für die Nutzung des Active Directory als Informationssystem sowie Bereitstellen eines Self-Service zum Passwortmanagement.

Hersteller
The Dot Net Factory
www.adselfservicesuite.com

Preis
50 Lizenzen der kompletten Suite kosten 595 US-Dollar, bei der Nutzung einzelner Module kosten 50 Lizenzen je Modul 350 US-Dollar. Es gibt Staffelpreise.

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

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

Darstellung der AD-Inhalte	7
Ändern von AD-Inhalten	6
Erstellen individueller Ansichten	6
Passwortwiederherstellung	8
Stabilität und Design der GUI	4

Dieses Produkt eignet sich

optimal für Unternehmen, die umfassende Informationen im Active Directory speichern und diese Daten allen Anwendern zugänglich machen wollen sowie einen Self-Service für das Passwortmanagement anstreben.

bedingt für Unternehmen, die das Passwortmanagement nicht einsetzen wollen und das AD nur in begrenztem Umfang zur Speicherung von Attributen nutzen. Dann reicht es oft auch, wenn Anwender durch einen das AD nutzenden Mail-Dienst wie Exchange auf gespeicherte Benutzerdaten zugreifen können.

nicht in Fällen, wo kein Bedarf besteht, die AD-Inhalte den Anwendern zugänglich zu machen.

The Dot Net Factory AD Self-Service Suite 3.6

Im Test: Realtech theGuard! 7

Den Fehlern auf der Spur

von Thomas Bär

Wichtige IT-Komponenten im Unternehmensnetzwerk müssen von Monitoring-Lösungen rund um die Uhr überwacht werden. Fällt eine aus, so wird der Administrator umgehend über den Missstand informiert. Mit dem neuen theGuard! 7 fasst Realtech zahlreiche Funktionen zum Monitoring, Netzwerk-Management und Business Process Management zusammen. Dank "Root Cause Analysis" sollen Administratoren dabei Fehlern auf den Grund gehen können. Wie das funktioniert und welche Neuerungen Version 7 mitbringt, hat sich IT-Administrator für Sie angeschaut.

Eigentlich gehört die Fehler-Ursachen-Analyse, die deutsche Bezeichnung für "Root Cause Analysis", als wesentliches Instrument zum Repertoire der Unternehmensführung und ist somit originär kein Begriff aus der IT. Sie beschreibt die Erfassung von Fehlern, ihrer Ursachen und die statistische Auswertung dieser Daten, an die sich typischerweise eine Bewertung und abgeleitete Maßnahmen zur Reduktion weiterer Fehler und auch Kosten anschließen. Losgelöst von den in der Unternehmensführung gesammelten Erfahrungen in Bezug auf die Ursächlichkeiten der Fehler handelt es sich bei der "Root Cause Analysis" in der IT um die Fähigkeit einer Software, die Ursache eines Problems aufzuzeigen.

Sind beispielsweise in einem Unternehmen zwei Printserver über Kreuz mit zwei Switches verbunden und steuern zwei identische Drucker an, so ist der Geschäftsprozess "Druck" in diesem Fall erst dann in Gefahr, sofern eine der doppelt angelegten Komponenten ausfällt. Die Überwachung der Printserver, die Überwachung der Switches und das Monitoring der Drucker sind einzelne, eher technische Überwachungsaufgaben. Den Zusammenschluss der einzelnen Überwachungen in einen überwachten Geschäftsvorgang "Drucken" erlaubt die "Root Cause Analysis". Da die Komponenten grafisch dargestellt werden, reicht ein einziger Blick auf die beteiligten Komponenten, um als Administrator sagen zu können, warum der Prozess nicht mehr funktioniert. Um jedoch den Ausfall oder die Gefährdung eines Geschäftsprozesses überhaupt über eine Software ermitteln zu können, ist es erforderlich, die darunterliegende technische Ebene zu überwachen.

Überwachung für heterogene Landschaften

Das Modul "theGuard! NetworkManager" als Management-System für heterogene IT-Netzwerke überwacht und kontrolliert Netzwerk- und Systemkomponenten wie Router, Switche, Firewalls, Server, PCs oder Drucker von unterschiedlichen Herstellern. Im Gegensatz zu herstellerspezifischen Management-Systemen, wie sie oft als Dreingabe zur Hardware mitgeliefert werden, ist der NetworkManager von vornherein dafür ausgelegt, heterogene Systemlandschaften abzubilden. Standard-Komponenten werden über Standard-Schnittstellen wie SNMP angesprochen. Soll die Software weitere, herstellerspezifische Funktionen nutzen, bietet Realtech sogenannte "Produktspezifische Module" (PSMs). Eine aktuelle Übersicht der angebotenen PSMs findet sich unter [1].

theGuard! NetworkManager bietet dem Anwender einen grafischen Überblick über das Netzwerk, erkennt weitgehend automatisch die physikalische sowie logische Netzwerk-Topologie und dokumentiert jedes Netzwerk-Ereignis aktuell und dauerhaft. Alle von NetworkManager gesammelten Daten werden in einer offenen Datenbank abgelegt und sind über dokumentierte Schnittstellen für andere Applikationen zugänglich.

Nach der Inbetriebnahme schneller Überblick aller Komponenten

Während des Ersteinrichtungsvorgangs prüft der Installer alle Abhängigkeiten und bricht den Vorgang bei einer fehlenden Softwarekomponente ab. Diese Vorgehensweise erspart dem Administrator die spätere

Systemvoraussetzungen und Testumgebung

TheGuard! setzt auf einem aktuellen Windows Server als Betriebssystem auf. Bei unserer Testmaschine handelte es sich um einen unter VMware virtualisierten Windows Server 2008 R2 SP1 in deutscher Sprache mit zwei zugewiesenen 2,67 GHz Xeon-CPUs, 4 GByte Arbeitsspeicher und einer 32 GByte großen Festplatte.

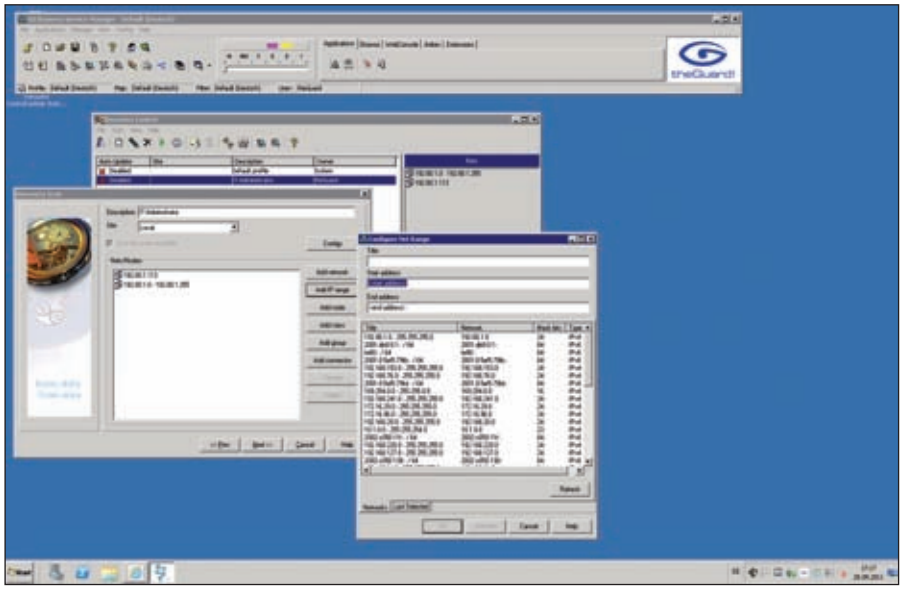


Bild 1: Die "Discovery Scans" ersparen dem Administrator die manuelle Zusammenstellung der im Netzwerk aktiven Geräte

Suche nach möglichen Fehlerquellen. Als Datenbanksystem setzt theGuard! typischerweise auf eine Microsoft SQL-Installation. In kleineren Umgebungen kann sich die Datenbank-Installation auf der lokalen Maschine befinden. Für große Umgebungen lässt sich der Datenbankserver auf einer separaten Maschine betreiben, wobei zwischen Applikations- und Datenbankserver explizit auf eine dedizierte Netzwerkverbindung hingewiesen wird.

Nach der Installation besteht ein erster Schritt darin, die gewünschten Netzwerkkomponenten ausfindig zu machen. Dazu verwendet der Administrator den Punkt "Discovery". Bevor mit der automatischen Erkennung begonnen wird, sind zunächst wichtige Informationen zum IP-Adressbereich, DHCP-Bereich, zur DNS-Namensauflösung und SNMP-Community-Informationen einzugeben. Praktischerweise lassen sich für die SNMP-Communities mehrere Einträge hinterlegen – das Programm versucht mit allen Einträgen, Informationen zu gewinnen. In Abhängigkeit zur Größe des Netzwerks finden sich nach kurzer Zeit alle Netzwerkgeräte wie Router, Server, Switches oder Drucker in der Oberfläche der Software wieder.

Die gefundenen Nodes verknüpften wir im Test über die Software logisch miteinander. So entstand die Abbildung des realen Netzwerks. Diese Landkarten kann der Benutzer auf verschiedene Hintergründe legen – Weltkarte, Kontinente oder Staatenkarten liefert Realtech gleich mit. Individuelle Umgebungskarten oder Digitalfotos von Serverschränken konnten wir problemlos per Bitmap-Datei einbinden.

Wird das Hauptprogramm gestartet, erscheint im oberen Bereich des Monitors eine Menüleiste mit allen Befehlen und eine zentrale Statusanzeige. In dieser Statusanzeige stellte die Software uns alle aktuellen Geschehnisse gruppiert in sieben unterschiedliche Prioritätsstufen, von "Hinweis" bis "Kritisch", dar. Direkt unterhalb der sieben farbigen Kästchen, die bei Eintreten eines Ereignisses zu blinken beginnen und so die Aufmerksamkeit des Benutzers auf sich ziehen, findet sich ein Schieberegler. Mit Hilfe dieses Reglers wird ein Ereignisfilter erhöht oder abgesenkt. Angesichts der Masse von Informationen, die bereits ein gutes Dutzend Netzwerkgeräte produziert, ist so eine Beschränkung auf das Wesentliche möglich.

Reports schnell gefiltert

Neben der reinen Windows-basierten Benutzeroberfläche bietet theGuard! eine Webkonsole für den Zugriff auf Reports oder Statusinformationen auch ohne lokale Installation. Besonders gefallen haben uns die schnell zu setzenden Filter, mit denen sich die Ansicht mit wenigen Klicks auf die gesuchten Elemente begrenzen lässt. Ganz neu mit der Version 7 ist die so genannte Windows Presentation Foundation-Oberfläche (WPF), die langfristig die bisherige Webkonsole und die traditionelle EXE-Datei ablösen soll. Aktuell bietet sich die WPF für Administratoren und Benutzer im Tagesgeschäft zur Problemanalyse oder Fehlersuche an.

Die Einrichtung von Netzwerkgeräten und die Definition von Business Views geschieht nach wie vor über die lokale Konsolensoftware. Im Detail haben die Entwickler bei Realtech viele Verbesserungen eingearbeitet. Die Mischung aus Filter und Gruppierung in jeder Tabellenansicht ermöglicht dem Benutzer, die gewünschten Informationen in kürzester Zeit zu selektieren, ohne einen Report anlegen zu müssen. Optisch ist die WPF-Oberfläche State of the art – veränderten wir etwa eine grafische Darstellung, flogen die gezeigten Elemente mit wachsender Beschleunigung an ihren neuen Darstellungsort - die Darstellung bleibt also immer identisch (WEB und LOKAL).

Neben der Prüfung der Erreichbarkeit eines Netzwerkgeräts mit Hilfe eines PING-Befehls gewinnt theGuard! weiterführende Informationen über die Protokolle SNMP 1 bis 3 und deren Erweiterung RMON. Netflow-Informationen werden, verknüpft mit SNMP-Daten, ebenfalls zur Analyse verwendet und erlauben so eine zentrale Übersicht der Netzwerkbewegungen in Echtzeit.

Granulare Regeln und Steuerung

Wie die Software auf Über- oder Unterschreiten von definierbaren Schwellenwerten reagieren soll, kann der Administrator sehr genau entscheiden. Unterschiedliche Reaktionsarten wie der Versand einer E-Mail, die Erstellung von Datenbankeinträgen, veränderte Poll-Befehle oder gezielte Remedy-Service-Aktionen sind möglich. Die wichtigste Aktion als Folge eines entstandenen Fehlers ist zunächst einmal dessen Protokollierung. In vielen Fällen dienen schon allein die Protokolle der Netzwerkmanagementsoftware und die Ereignisprotokolle von Servern dem Administrator zur Eingrenzung eines Problems. Ohne derlei Daten befindet sich die IT förmlich im Blindflug. Die gesammelten Meldungen an den Benutzer werden im Logbuch von theGuard! mitgeschrieben und sind vom Nutzer zu bestätigen. So ist sichergestellt, dass

die Meldung überhaupt jemand zur Kenntnis nimmt. Bis zu dieser Bestätigung blinken die ungesehenen Fehlermeldungen dauerhaft vor sich hin.

Neben der Überwachung des Status und der automatisierten Informierung des IT-Personals eignet sich das Programm ebenfalls zur zentralen Steuerung. Sind die entsprechenden MIB-Dateien der Aktivkomponenten eingebunden, ist nach einem Doppelklick auf eine Komponente – beispielsweise einem Switch – deren Gestalt im Programmfenster abgebildet. Auch der Status der LEDs wird in der Visualisierung wiedergegeben. Durch Anklicken der Ports kann der Benutzer Befehle wie die Port-Deaktivierung direkt über theGuard! abwickeln, ohne dass dieser in die produktspezifische Software oder Weboberfläche wechseln müsste. Sollen Windows-Maschinen überwacht werden, so ist entweder die Aktivierung eines SNMP-Agents erforderlich oder es wird WMI (Windows Management Instrumentation) verwendet.

Ursachenforschung dank Prozessanalyse

Vor gut fünf Jahren stellte Realtech erstmals mit der Version 6.1 den "Business Process Manager" (BPM) vor. Hierbei handelt es sich um eine logische Verknüpfung der eher technischen Infrastruktur mit den Geschäftsprozessen des Unternehmens. BMP liefert, quasi im Vorbeigehen, zudem die von vielen Administratoren gesuchte Antwort auf die Frage nach der eigentlichen Ursache für Ausfälle. Insgesamt bietet die Darstellung der Geschäftsprozesse im Zusammenspiel mit der Infrastruktur der IT einen großen Vorteil. Einerseits verdeutlicht dies die Zusammenhänge von Einzelsystemen innerhalb des Gesamtsystems, andererseits ist die grafische Darstellung der Abhängigkeiten von Systemen für das nicht-technische Personal einfacher nachzuvollziehen. Der theGuard! BPM ist komplett in die Oberflächen des NetworkManagers eingebunden und findet sich als Zweig in der Menü-Baumstruktur. "Business View"-Prozesse, die im BMP beschrieben sind, veranlassen die herkömmlichen Überwachungselemente von theGuard!, mit sieben Farbwerten auf Missstände zu reagieren. Es macht somit keinen Unterschied, ob ein physikalisch existierendes System einen Ausfall meldet oder ob sich ein vom Benutzer definierter Prozess außerhalb der geplanten Parameter befindet.

Bevor jedoch ein Geschäftsprozess mit theGuard! auf seine Funktionalität hin automatisiert überwacht wird, müssen erst einmal die Stammdaten der Netzwerkinfrastruktur erfasst sein. Diese Daten, die der BPM als Grundlage für die Verarbeitung benutzt, kommen aus der so genannten CMDB (Configuration Management Database). Dies sind die Informationen, die zuvor über den Network Manager gesammelt wurden. Für viele Drittsysteme wie SAP via SAP-Control, JMX, Microsoft Active Directory, Microsoft Exchange, Microsoft SQL oder Java-basierte Systeme über JMX mit Tomcat bietet der Hersteller fertige Business-Connectoren, die detaillierte Informationen sammeln. Aktuell in der Entwicklung befinden sich Connectoren zu VMware ESX, wahlweise mit VCenter oder direkt über die einzelnen Server, zu Citrix-Produkten und zu Microsofts Hyper-V.

Die normalisierten Daten der CMDB verarbeitet der BPM gemäß den Definitionen des Administrators weiter. Wurden bisher Programme wie theGuard! für die reine Überwachung der Funktion von Geräten und die Prüfung derer Leistungsdaten verwendet, so geht BPM einen Schritt weiter. Faktisch handelt es sich bei der Funktionalität BPM um eine weitere Ebene in der Betrachtung durch die IT. Um beispielsweise sicherzustellen, dass Kunden nach einem Anruf im Support eine Bestätigungs-E-Mail erhalten, was ein simpler Geschäftsprozess ist, ist eine möglicherweise umfangreiche technische Umgebung notwendig. Dieser Prozess basiert auf dem Funktionieren des E-Mailservers, des Storage-Systems, der Datenbank mit den Kundendaten, der möglicherweise drei Switches, an denen die Maschinen angeschlossen wurden, des Backbones, der die Systeme verbindet, des Internet-Routers und dem Funktionieren der Internetleitung des Providers selbst.

Grafische Erstellung eigener Geschäftsprozesse

Die Erstellung der eigenen "Business Views" im NetworkManager durch den IT-Verantwortlichen ist relativ simpel und erfordert in erster Linie vorheriges Nachdenken. Ein Geschäftsprozess wird, wie ein Netzwerkgerät, auf einer Überwachungskarte positioniert. Mit welcher Symbolik ein Geschäftsprozess bei theGuard! dargestellt wird, ist Geschmackssache des Anwenders. Bei Bedarf kann dieser eigene Bilder als Bitmap-Datei einbinden.

Im nächsten Schritt werden die Elemente, die für den Prozess von Bedeutung sind, hinzugefügt. Dabei kann es sich um ein Netzwerkinterface, einen Dienst, einen anderen Business Process oder jedes andere

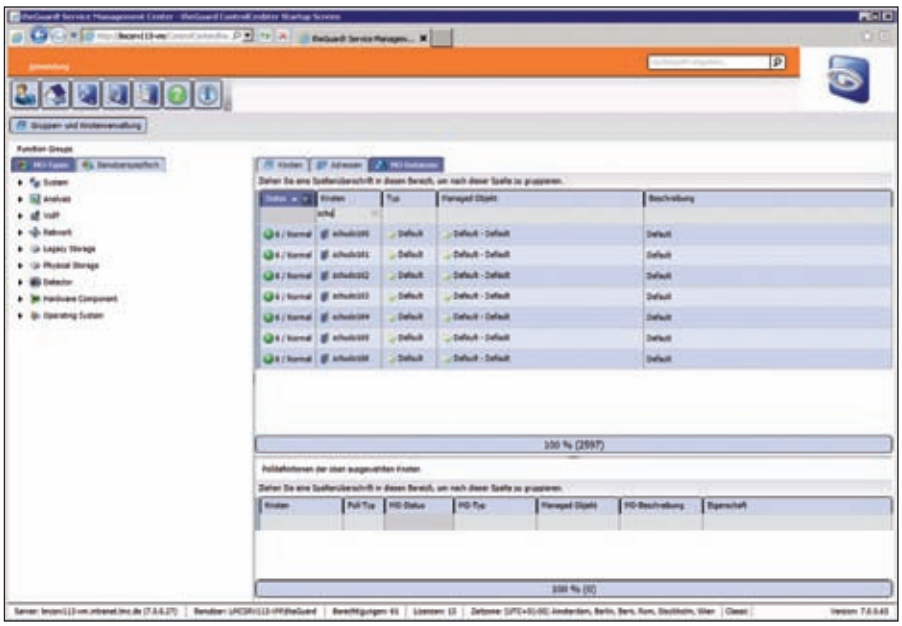


Bild 2: Die neue Weboberfläche von theGuard, basierend auf WPF-Technik, erlaubt freies Filtern und Gruppieren von Listen – so wird die gewünschte Datenmenge zügiger dargestellt

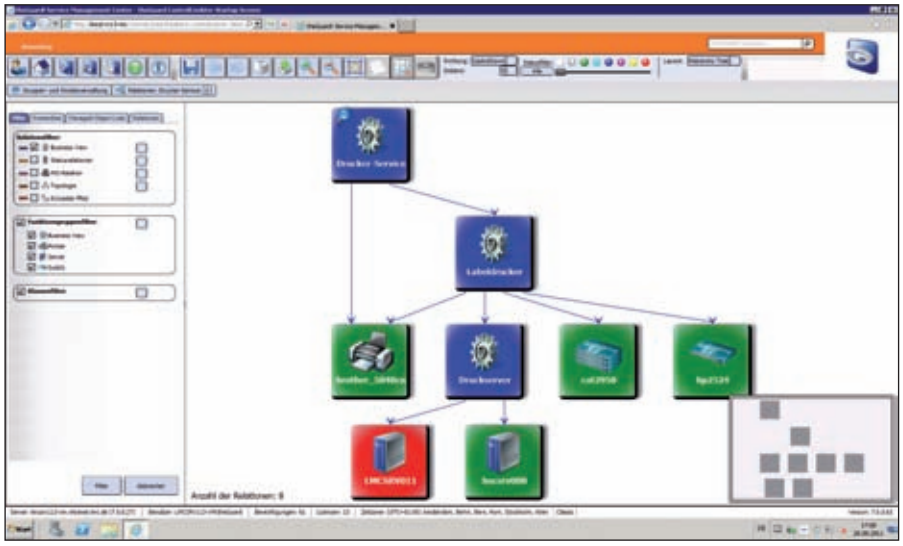


Bild 3: Selbsterklärende Grafiken wie die "Root Cause Analyse" der Druckerüberwachung helfen Admins bei der Fehlersuche

Objekt aus dem NetworkManager handeln. Die einzelnen Komponenten lassen sich anschließend in einer Reihenfolge ineinander mit verschiedenen Logikbefehlen wie "ist gleich", "ist ungleich", "größer als", "kleiner als" oder "im Durchschnitt größer als" verschachteln. Die zu vergleichenden Werte sind die bei theGuard! bereits bekannten sieben Statuswerte "Fatal", "Critical", "Minor", "Warning", "Harmless", "Normal" und "Informational". Das Ergebnis dieser Prüfung ist ebenfalls einer dieser sieben Statuswerte, die entweder fix vom Benutzer vorgegeben oder als Resultat des Prozesses (schlechtester oder bester Wert) ausgewertet wurden.

Ist beispielsweise die Internetverbindung gestört, da der Router kein Signal auf dem externen Interface findet, so ist dies für den Prozess "E-Mail-Versand" erst dann ein tatsächliches Problem, sofern eine hoffentlich eingerichtete Sekundärverbindung ebenfalls gestört ist. Im BPM würde der Wechsel der ersten Prüfung zu "Kritisch" zur möglichen zweiten Prüfung führen, ob denn die Sekundärverbindung noch aktiv ist. Ist dies der Fall, so würde das Ergebnis der Prozess-Prüfung weiterhin als "Normal" betrachtet. Es handelt sich bei diesen Prüfungen somit um eine Korrelation verschiedener Überwachungen.

[1] Angebotene "Produktspezifische Module"
BBT31

Link-Codes

Aussagekräftige Ereignis-Korrelation

In der Korrelationsansicht – der Zusammenfassung, in der die aufeinander aufbauenden Eigenschaften in einer logischen Verknüpfung zueinander dargestellt werden – findet sich ein für die Fehleranalyse sehr wichtiges Auswahlfeld: der Zeitpunkt. Standardmäßig zeigt das Korrelationsfenster den aktuellen Zustand eines "Business Views". Jeder Zeitpunkt, an dem sich eine Eigenschaft einer der beteiligten Komponenten verändert hat, wird protokolliert und erlaubt es dem Anwender, sich den Vorgang zu einem späteren Zeitpunkt erneut zu betrachten. Führte beispielsweise der Ausfall eines Internetrouters zur Unterbrechung des "E-Mail-Versand"-Prozesses, so wird in der grafischen Darstellung anhand des gängigen Farbmodells schnell klar, warum der Geschäftsprozess "E-Mail" unterbrochen wurde: der Router war defekt.

Diese Darstellung wird als "Root-Cause-Analyse" bezeichnet. Die gedankliche Verkettung, dass ein Router-Ausfall gleichzeitig den E-Mailversand lahmlegt, muss mit Hilfe von Programmen wie dem BPM von theGuard! nicht mehr allein durch den Administrator geschehen. Aufgrund der gewonnenen Erkenntnisse ist das "Business Process Management" in der Lage, die unterschiedlichsten Aktionen anzustoßen. Auch hier steht die übliche Palette von Benachrichtigungen zur Verfügung, wie der Versand von E-Mails, Logfile- oder Datenbankeinträge, veränderte Poll-Überwachungsbefehle oder das Generieren einer Trouble-Ticket-Meldung.

Fazit

TheGuard! von Realtech besticht als Überwachungs- und Analyse-Software mit einer großen Anzahl von Funktionen, einer ausgereiften technischen Grundlage und einem in sich stimmigen Konzept. TheGuard! ist mehr als eine reine Netzwerküberwachungssoftware: Hier wird Monitoring und Business gleichermaßen überwacht, was die Nutzbarkeit in der Praxis deutlich verstärkt. *(dr)*

Produkt
Software zur Überwachung von Netzwerkkomponenten und zur Fehleranalyse.

Hersteller
Realtech
www.realtech.de

Preis
Die Preise beginnen ab rund 9.520 Euro für 500 Nodes beim theGuard! Network Manager. Für 5.000 Nodes verlangt der Hersteller zirka 23.800 Euro.

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

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

Geräteerkennung	9
Root-Cause-Analyse	9
Netzwerk-Monitoring	9
Business View-Definition	8
Einrichtung und Bedienung	7

Dieses Produkt eignet sich

optimal für Unternehmen, die eine sehr hohe Anzahl von Netzwerkkomponenten besitzen, die in einer sehr individuellen oder eher unübersichtlichen Art und Weise verknüpft sind.

bedingt für Unternehmen mit sehr wenigen Aktivkomponenten oder Geschäftsautomatismen, die es zu überwachen gilt.

nicht für Unternehmen, deren Prozesse nicht auf automatisierten IT-Systemen basieren.

Realtech theGuard! 7

1&1 WEBHOSTING

INKLUSIVE CLICK & BUILD APPS!

Bei 1&1 treffen über **20 Jahre Webhosting-Erfahrung** auf modernste Technik in deutschen **Hochleistungs-Rechenzentren.** Mehr als **1.000 IT-Profis** entwickeln unsere hochwertigen Lösungen permanent weiter. 1&1 bietet Ihnen alles, was Sie für Ihren **professionellen Internetauftritt** brauchen:

✓ **65 kostenlos installierbare Click & Build Applikationen**
Joomla, Wordpress, Gallery und viele Apps mehr!
Inklusive Software- und Sicherheits-Updates.

✓ **Marken-Design-Software**
z. B. Adobe Dreamweaver®, NetObjects Fusion® 1&1 Edition

✓ **Doppelte Sicherheit**
paralleles Hosting Ihrer Website in zwei Hightech-Rechenzentren an verschiedenen Orten

✓ **24h-Profi-Hotline**
und kostenloser E-Mail-Support.

AKTIONEN BIS 31.12.11

WEBSITE
1&1 DUAL PERFECT

- **6 DOMAINS INKLUSIVE**
- **5 GB** Webspace
- **UNLIMITED** Traffic
- **UNLIMITED** Click & Build Apps

6 MONATE FÜR
0,– €/Monat*
danach 9,99 €/Monat*

.DE UND .INFO DOMAIN
0,29 €
im Monat,
danach ab 0,49 €/Monat.*

Weitere Spar-Aktionen im Internet.

1&1

Internet made in Germany

0 26 02 / 96 91
0800 / 100 668

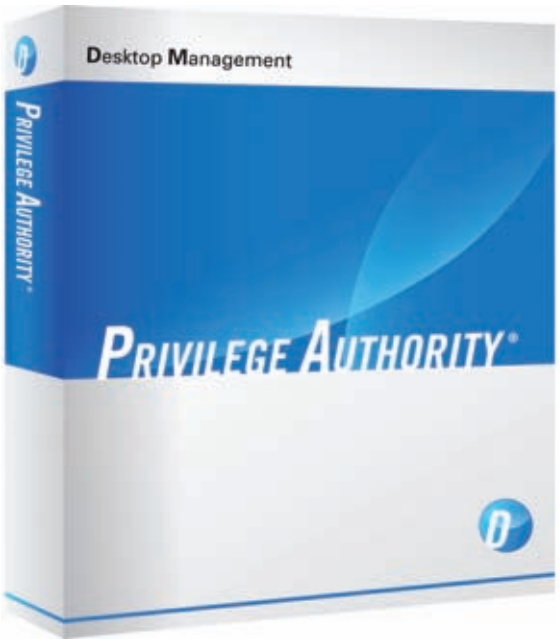
www.1und1.info

* 1&1 Dual Perfect, 6 Monate 0,– €/Monat, danach 9,99 €/Monat. Einmalige Einrichtungsgebühr 9,60 €. Software wird zum Download bereitgestellt.
.de und .info Domain 1 Jahr 0,29 €/Monat, danach .de 0,49 €/Monat und .info 1,99 €/Monat. Keine Einrichtungsgebühr. Alle Pakete 12 Monate Mindestvertragslaufzeit. Preise inkl. MwSt.

Im Kurztest: ScriptLogic Privilege Authority 2.5

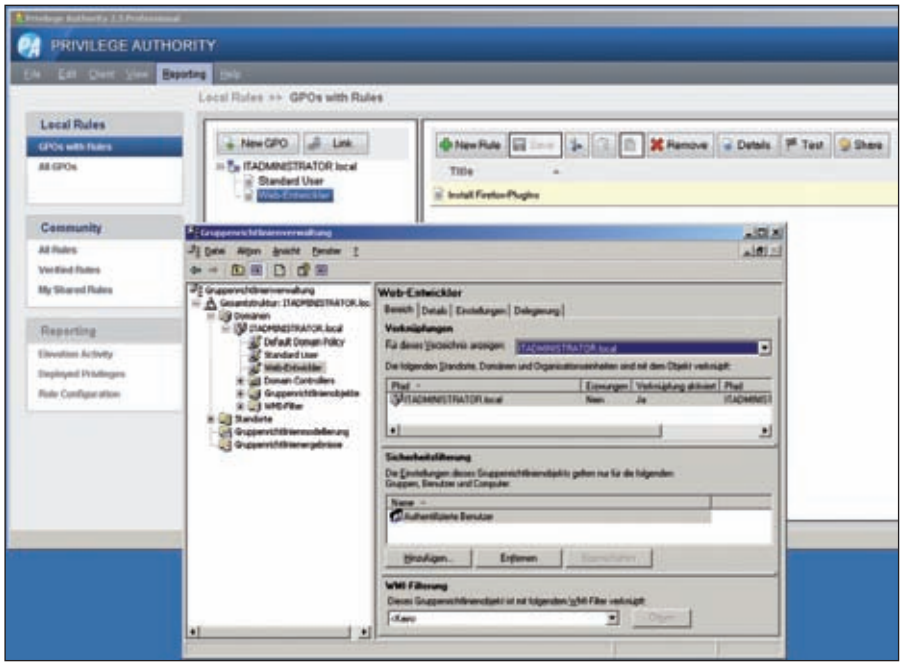
Privilegien statt Rechte

von Sandro Lucifora



Viele Anwendungen funktionieren nicht ohne administrative Berechtigungen – entweder weil sie Zugriff auf spezielle Admin-Funktionen benötigen oder weil sie nicht für eingeschränkte Benutzerrechte entwickelt wurden. Dies widerspricht aber meist den Prinzipien sicherer Nutzerverwaltung, da die Anwender im Netzwerk nur eingeschränkte Rechte haben sollten. Einen Ausweg aus diesem Dilemma will Privilege Authority bieten. Mit der Software legt der Administrator über zentrale Regeln fest, welche Bereiche der Anwender selbst verwalten darf – ohne dem Benutzer volle lokale Admin-Rechte erteilen zu müssen. Wir haben getestet, ob die granularen Zugriffsrechte greifen und sensible Bereiche weiterhin außer Reichweite der Nutzer bleiben.

Voraussetzung für den Einsatz von Privilege Authority ist die Microsoft Group Policy Management Console 5.2 oder höher. Nachdem diese und Privilege Authority (PA) selbst aufgespielt waren, konnten wir direkt erste Regeln anlegen. Dabei berücksichtigt PA auch mehrere Domänen. Zunächst strukturierten wir die neuen GPOs in Gruppen, etwa Abteilungen, Niederlassungen oder Anwendungsgebiete. Innerhalb dieser Gliederung wird eine neue Policy erstellt. Der Assistent führte uns dazu durch die einzelnen Schritte. Es boten sich uns vier Möglichkeiten, um die Regeln zuzuordnen. Wird eine bestimmte ausführbare Datei oder ein EXE-File aus einem definierten Pfad aufgerufen, kann es zum Anheben der Berechtigung kommen. Dies ist auch für die User-Berechtigung auf einen kompletten Pfad möglich. Um zum Beispiel Adobe-Updates für den Acrobat Reader und Flash zu erlauben, konnten wir die Steuerung für den Aufruf eines ActiveX-Moduls über eine URL festlegen. Eine weitere Option ist die Bindung der Regel an den "Publisher Name", den Hersteller des Zertifikates. Eine Kombination aller vier Möglichkeiten stellt kein Problem dar und ist oft sinnvoll.



Nach dem Verlinken der neuen Regeln sind diese als Gruppenrichtlinien im Active Directory verfügbar

Einfache und sichere Rechtevergabe

Im Wizard gaben wir dann an, für welches Windows-Betriebssystem die zuvor festgelegte Regel greift. Hier fehlt uns gerade für Windows 7 die Option, zwischen 32 und 64 Bit zu unterscheiden. Ein weiterer Schritt innerhalb des Assistenten legt fest, wann genau die Regel zum Zug kommt. So konnten wir diese einzelnen Computern und Computergruppen oder auch Benutzern und Benutzergruppen zuordnen. Mit IF, AND und OR-Operatoren ist eine genaue Definition möglich. Über

die Testfunktion haben wir vor dem Verlinken in die Gruppenrichtlinien die Funktion der Regel überprüft.

Im Test konnten wir klassische Rechte-Problematiken wie das Online-Update von Adobe-Produkten oder die Aktualisierung von Java lösen. Des Weiteren haben wir durch eine Policy der Benutzergruppe "Buchhaltung", nicht aber den Auszubildenden der Gruppe, Rechte auf die Ausführung der Accounting-Software in einem Netzwerkpfad erteilt. Ein weiteres Testszenario war Adobe InDesign, das nur über eine englischsprachige Oberfläche verfügt, wenn der Anwender keine administrativen Rechte und somit keinen Zugriff auf die Sprachdateien hat. Wir haben diese Einschränkung mit einer Gruppenregel gelöst, ohne dass der User sonstige Admin-Rechte erhielt.

Lizenzierung pro Client

Die Software besteht lediglich aus dem Management-Tool, das auf dem Active Directory-Server installiert wird. Um die mit PA erstellten Regeln im Netzwerk zu aktivieren, ist über die Link-Funktion die neue GPO in der Domäne oder der OU zu verlinken. Ab diesem Zeitpunkt erhält jeder Arbeitsplatz nach dem Login die Regeln übermittelt.

Die Lizenzen beziehen sich auf die Anzahl der Arbeitsplätze, für die Administratoren mit PA Regeln erstellen. Die Lösung ist nur auf Englisch erhältlich und unterstützt Windows ab XP Service Pack 2 einschließlich Windows 7 und Server 2003 / 2008. Erforderlich sind das .NET Framework 2.0 und die Group Policy Management Console.

Fazit

Privilege Authority erleichtert Administratoren die Umsetzung von Standardaufgaben wie die Installation eines Adobe Reader-Updates oder die Freigabe eines ActiveX-Applets. Die Software kann Benutzer für einzelne Applikationen mit höheren Rechten ausstatten, indem sie Regelsätze nutzt, die mit Gruppenrichtlinien verknüpft sind Standardregeln für einige Anwendungen sind bereits über das Forum zu beziehen, wobei sich die meisten allerdings auf englische und nicht aktuelle Software beziehen. Sie dienen aber als gute Grundlage, um eigene Regeln zu erstellen. Insgesamt überzeugt die Software durch ihre einfache und dennoch sehr effektive Arbeitsweise. Sie ist prädestiniert, die Probleme mit Benutzerrechten in den Griff zu bekommen, die fast alle Administratoren haben. *(ln)*

Mit der "Community Edition" bietet ScriptLogic eine kostenlose Variante seines Werkzeugs zur Rechtevergabe zum Download an. Bei den Basisfunktionen des Tools, dem begrenzten Heraufstufen von Rechten in Bezug auf spezifische Applikationen oder Prozesse, muss der Nutzer keine Abstriche machen. Der Hauptunterschied zur kostenpflichtigen Variante besteht jedoch vor allem im Nichtvorhandensein jeglicher Reporting-Funktionen. Auch was das Erstellen von Server- oder Betriebssystem-spezifischen Regelsätzen betrifft, bietet die freie Version keine Unterstützung. Zudem müssen Test-Nutzer auf Support verzichten.

Abgespeckte Freeware-Version

Produkt

Programm zur granularen Rechtevergabe in Active Directory-Umgebungen.

Hersteller

ScriptLogic Corporation
www.scriptlogic.com

Preis

Das Startpaket mit zehn Clients kostet 107,50 Euro. Jede weitere Lizenz ist für 10,75 Euro zu haben.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Umsetzung	7
Handhabung	7
Konfigurationsaufwand	10
Zuverlässigkeit	6
Kosten/Nutzen	7

ScriptLogic Privilege Authority 2.5

Wenn alles auf dem Kopf steht...

Bringen Sie Ordnung in Ihr Druckerchaos!

steadyPRINT
Zentrales und ausfallsicheres Druckermanagement.

- Zentrales Management der kompletten Druckerumgebung
- Ausfallsicherheit für Druckserver
- Online Job-Überwachung einzelner Drucker
- Echtzeitmapping von Druckerverbindungen
- Domänenübergreifende Druckerzuweisung

www.steadyprint.com

Im Kurztest: Strato HiDrive

Ab in die Wolke

von Sandro Lucifora

Eine gute Backupstrategie berücksichtigt auch Vandalismus, Wasserschäden oder Feuer. Dazu müssen die Backupmedien aus dem Gebäude gebracht werden, in denen die EDV steht – doch erfahrungsgemäß wird dies vor allem bei kleineren und mittleren Unternehmen vernachlässigt. Die primäre Anwendung unseres Testprodukts HiDrive ist daher das Daten-Backup in die Cloud oder auch das Vorhalten einer Backup-Kopie.

HiDrive stellt einen exklusiv reservierten Speicherplatz auf einem Netzwerkspeicher dar. Zwischen 5 GByte und 5 TByte kann der Speicherplatz in der Cloud bei Strato betragen. Neben der Speicherplatzgröße unterscheiden sich die Pakete in der Anzahl der Benutzerkonten als auch den Freigabelinks und der Form des Backups. Im Kasten "HiDrive-Pakete" finden Sie eine entsprechende Übersicht. Laut Anbieter wird das Strato-Rechenzentrum in Deutschland betrieben und unterliegt somit dem deutschen Datenschutzrecht.

HiDrive als Festplatte nutzen

Nach dem Login begrüßt uns eine klar strukturierte und intuitiv verständliche Benutzeroberfläche, die in die Bereiche "Übersicht", "Dateimanager" und "Einstellungen" gegliedert ist. Der direkteste Weg, Daten auf der HiDrive zu speichern – der immer und überall funktioniert – ist über den Web-basierten Dateimanager. Im Internetbrowser gestartet, navigieren wir im Verzeichnis, legen Verzeichnisse an und laden bei Bedarf Daten auf den lokalen Rechner herunter.

Für den Alltag und an den eigenen Geräten ist das Einbinden ins System als "normale" Festplatte besser. Das ist sowohl auf Windows-, Mac- als auch auf Linux-Computern möglich. Die HiDrive unterstützt dazu die Protokolle SMB/CIFS, WebDAV, S/FTP, FTPS, rsync, SCP und OpenVPN. Über die Benutzeroberfläche erhielten wir eine gute Hilfestellung zur Einbindung. Nach der Auswahl des Kontos, des Betriebssystems und des Protokolls zeigt die Webseite eine gute Schritt-für-Schritt Anleitung an. Web-DAV und SMB/CIFS konnten wir über eine verschlüsselte Verbindung mit SSL einrichten. Unter Linux erstellten wir für rsync einen OpenSSH-Schlüssel, den wir ebenso für die SFTP-Verbindung einsetzten.

Wir haben HiDrive unter Windows Server 2003 und 2008, Windows 7 sowie SuSE- und Ubuntu-Linux mit den verschiedenen Protokollen verbunden. Wir stellten die Verbindungen sowohl "manuell" her als auch über die Strato-Software für Windows 7 64 Bit. Mit Letzterer konnektierten wir HiDrive über eine VPN-Verbindung. Ein Vorteil der Software ist, dass diese Lösung keine Administratorrechte auf dem Computer benötigt. Daher kann sie ebenso auf Fremdrechnern als auch Netzwerk-Clients ohne Admin-Rechte eingesetzt werden.

Problem: SMB/CIFS

Einige Router erlauben den direkten Zugang über SMB durch die eigene Firewall nicht. Da auch wir das Problem mit einer Fritz!Box hatten, haben wir – wie von Strato empfohlen – SMB/CIFS verschlüsselt verbunden und dazu OpenVPN eingerichtet. Zusätzlich findet sich unter [1] eine Anleitung, wie durch eine manuelle Veränderung der Konfigurations-Datei der Fritz!Box doch SMB/CIFS möglich ist.

Komfortabler Datenaustausch

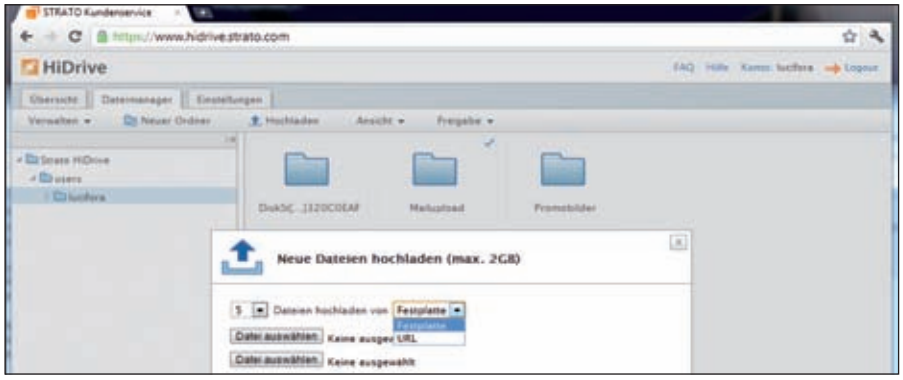
Abteilungen müssen oft Daten austauschen, was HiDrive über verschiedene Wege unterstützt. In der HiDrive-Benutzerverwaltung richteten wir mehrere Benutzer für die Online-Festplatte ein, denen wir Lese- oder Lese- und Schreibrechte für den gemeinsamen Ordner "public" erteilten. Vermisst haben wir hier eine automatische Versionierung der Dateien, um gegebenenfalls alte Versionsstände wiederherzustellen. Für externe Auftragnehmer ohne Userrechte auf HiDrive lässt sich der Datenaustausch über den "Freigabelink", die Funktion "Upload-Freigabe" und "Mailupload" realisieren.

Über den Freigabelink stellten wir Daten zum Download bereit. Wir wählten im HiDrive-Dateimanager eine Datei aus und gaben an, wie viele Tage und für wie viele Downloads der Freigabelink verfügbar ist und ob für den Download ein Kennwort benötigt wird. Danach erstellte HiDrive einen kryptischen Freigabelink, den wir dem Empfänger zukommen ließen.

Für das Hochladen ohne Benutzerrechte auf HiDrive nutzten wir die Upload-Freigabe. Wenn zum Beispiel Bilder und Videos zu groß sind, um sie per E-Mail zu verschicken, können Anwender diese über den Internetbrowser hochladen. Auch hier erzeugt HiDrive einen Short-Link

Verfügbare HiDrive-Pakete

Speicherplatz in GByte	User/Admin	Backup Control	Preis pro Monat bei einer Vertragslaufzeit von 24 Monaten
5	1/1		kostenlos
20	1/1	6 Wochen	1,49 Euro
100	1/1	6 Wochen	4,90 Euro
500	5/1	3 Monate	9,90 Euro
1.000	25/5	1 Jahr	39,90 Euro
2.500	60/10	2 Jahre	79,00 Euro
5.000	120/20	3 Jahre	149,00 Euro



Dateien lassen sich über den Browser von der lokalen Festplatte oder einer URL auf die HiDrive übertragen

auf eine komfortable Upload-Seite. Leider sind die Gültigkeit, die Anzahl maximaler Uploads und die Uploadgröße beschränkt. Bei beiden erzeugten Links für den Down- und Upload würden wir uns wünschen, dass sich die Down- und Upload-Seiten individualisieren lassen – zumindest mit Firmenlogo und Farben.

Eine Alternative kann auch der Mailupload sein, der Dateien per E-Mail empfängt und auf HiDrive ablegt. Uns hat dabei gefallen, dass die Gültigkeit der E-Mailadresse unbegrenzt sein kann. In der Konfiguration stellten wir fest, dass der Absender eine Empfangsbestätigung und der Empfänger – also wir – eine Eingangsbestätigung erhalten. Um die empfangenen Dateien besser zu sortierten, ließen wir je Absender einen Unterordner anlegen. Gut ist es, dass es keine Größenbeschränkung der Dateianhänge gibt. Die E-Mailadresse zum Empfang ist eine Kombination aus dem Benutzer- und Verzeichnisnamen sowie einer Strato-Domain. Mit der Benachrichtigungs-E-Mail wurden wir über den Eingang und die Anzahl der Dateien informiert. Zwar wurde auch der E-Mailbetreff und -Absender mitgeteilt, aber leider nicht der E-Mailtext mit übermittelt. Hier muss Strato noch nacharbeiten.

Bewährte Technologie für Backup und Archivierung

Sicherheit wird bei HiDrive groß geschrieben. Die Daten lassen sich nicht nur speichern, sondern auch über das Backup archivieren. Strato setzt dabei die aus dem Webhosting bekannte Technologie "Backup-Control" ein. Je nach gewähltem HiDrive-Paket werden die Daten über ein tägliches Backup bis zu drei Jahre aufbewahrt.

Die Backupregel haben wir für verschiedene Ordner unterschiedlich festgelegt und sogar ein Verzeichnis alle vier Stunden gesichert und diese Daten acht Wochen archivieren lassen. Durch Backup Control konnten wir jederzeit auf die letzten Versionsstände der Daten zurückgreifen und versehentlich gelöschte Dateien wiederherstellen.

Mobilität groß geschrieben

Um die Aussage einzuhalten, dass die Daten überall verfügbar sind, stellt Strato eine Vielzahl von Apps zur Verfügung. So konnten wir über die HiDrive App für Android Phone jederzeit auch unterwegs auf unsere Daten zugreifen, Texte und Tabellen lesen oder Dateien von der HiDrive auf dem Smartphone als Anhang per E-Mail versenden.

Einzelne Dateien ließen sich auch freigeben, doch Upload-Links oder ein Mailupload konnten wir hier nicht einrichten. Neben Android unterstützt der Hersteller auch Windows Phone 7 und das iOS des iPhone und iPad.

Fast wie eine lokale Festplatte

Nach der Einbindung von HiDrive unter Windows erfolgt der Zugriff fast so schnell wie auf eine lokale Festplatte - natürlich in Abhängigkeit der lokalen Internet-Anbindung. Da WebDAV keine stehenden Verbindungen aufbaut, waren erneute Anmeldungen in regelmäßigen Abständen erforderlich. Nach jeder Abfrage der Zugangsdaten baute der Server die Verbindung neu auf. Im Test haben wir mit der kostenlos erhältlichen HiDrive-Software verschlüsselte Verbindungen via SMB/CIFS aufgebaut und ein Laufwerk eingebunden. Dazu bedient sich der Anbieter der Lösung OpenVPN. Damit konnten wird dann über eine stehende Verbindung auf den Online-Speicher wie auf eine echte Festplatte zugreifen. Dabei ließen sich Dateien direkt öffnen und bearbeiten, ohne sie komplett herunterladen zu müssen.

Fazit

Die Strato HiDrive eignet sich sehr gut für den Einsatz in Unternehmen. Neben der Möglichkeit, sein Datenbackup auszulagern, sind auch die durchdachten Funktionen für die Zusammenarbeit in einer Gruppe im Arbeitsleben hilfreich. Die vielfältigen Verbindungs-Protokolle und mobilen Apps ermöglichen einen Datenzugriff von überall. *(jp)*

Produkt
Im Internet reservierter Speicherplatz, als Netzwerklaufwerk nutzbar.

Hersteller
Strato AG
www.strato.de
www.free-hidrive.com

Preis
siehe Kasten "Verfügbare HiDrive-Pakete"

Für HiDrive-Kunden bietet Strato zu einem Vorzugspreis lokale Netzwerkspeicher der Firma Synology an. Seit Ende September liefert Synology eine HiDrive App aus, mit der NAS-Daten auf HiDrive gesichert werden.

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

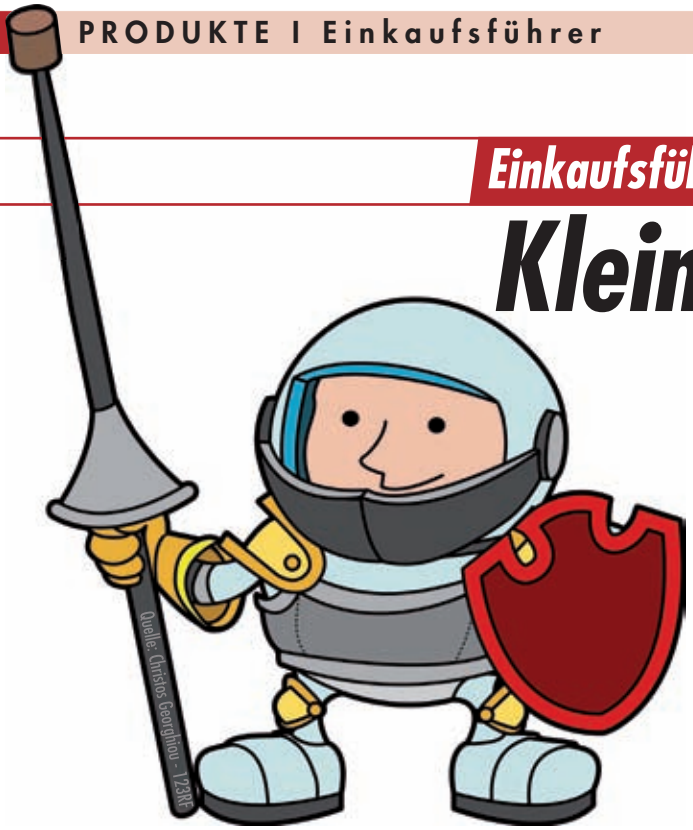
So urteilt IT-Administrator *(max. 10 Punkte)*

Umsetzung	7
Handhabung	7
Aufwand der Konfiguration	6
Zuverlässigkeit	7
Kosten/Nutzen	5

Strato HiDrive

[1] Anleitung zur Veränderung der Konfigurations-Datei der Fritz!Box bezüglich SMB/CIFS
BAT81

Link-Codes



Einkaufsführer: IT-Sicherheit für den Mittelstand

Klein, aber geschützt!

von Isabell Unseld

Der Mittelstand ist den gleichen Sicherheitsrisiken ausgesetzt wie internationale Konzerne. Der Unterschied liegt allerdings im Risikobewusstsein, den finanziellen Mitteln und in den daher angewendeten Schutzmechanismen – hier sind Großunternehmen dem Mittelstand in der Regel einige Schritte voraus. In diesem Einkaufsführer gehen wir darauf ein, worauf Verantwortliche im KMU-Bereich in Bezug auf Sicherheit achten sollten und welche Bereiche ihres Netzwerkes eines besonderen Schutzes bedürfen.

Ein Großteil der mittelständischen Unternehmen in Deutschland ist bescheiden: Sie können sich nicht vorstellen, warum ausgerechnet sie ins Visier von Hackern rücken könnten. Dabei sind Patente, Kundendaten, Entwicklungspläne oder die digitale Buchhaltung von enormer Bedeutung für das Fortbestehen eines Unternehmens. Effektive Schutzmaßnahmen sind deshalb unverzichtbar.

Gleiche Probleme, bescheidene Mittel

Kleine und mittelständische Unternehmen müssen sich gegen dieselben Bedrohungen verteidigen wie ein Großkonzern. Punktuelle Schutzverfahren reichen gegen mittlerweile sehr ausgereifte und vielschichtige Attacken nicht mehr aus. Dem Mittelständler stehen aber bei gleicher Problemlage sowohl personell wie auch finanziell wesentlich geringere Ressourcen zur Verfügung. Mit den gegebenen Mitteln das Bestmögliche an Schutz sicherzustellen, ist daher das Ziel für KMU-Betriebe.

Größtmögliche Effektivität setzt voraus, Kompatibilitäts- und Wartungsprobleme, die sich möglicherweise durch den Einsatz mehrerer Einzellösungen von verschiedenen Herstellern ergeben, durch die Verwendung einer umfassenden Lösung zu verringern. Eine weitere Steigerung der Sicherheitseffektivität wird durch bessere Transparenz der IT, maximale Kontrolle und umfassende Einblicke in die Sicherheitslage des Unternehmens erreicht. Eine zentrale Steuerung vereinfacht zusätzlich die Überwachung, Wartung und das Reporting. Das schließt auch eine Auslagerung der IT-Sicherheit als Security-as-a-Service an eine dritte Partei mit ein.

Diese Systeme müssen Sie schützen

Einfallstore für Attacken gibt es viele. Schnell werden dabei überaus wichtige Bereiche übersehen:

Wirksamer Endgeräteschutz

Das Spektrum reicht vom Desktop über Laptops und Tablet PCs bis hin zu Smartphones, auf denen mittlerweile eine Fülle an Daten gespeichert ist, die sensibel sein können. Außerdem sind gerade mobile Geräte, die zum Beispiel an ungesicherten Hotspots eingesetzt werden, die schwächsten Glieder der Unternehmenssicherheit. Folgende grundlegenden Sicherheitsfunktionen für Endgeräte, die Online-Bedrohungen nur im begrenztem Maße ausgesetzt sind, sollten in jedem Fall vorhanden sein:

- Anti-Virus
- Spyware-Schutz
- Sicheres Surfen
- Anti-Spam
- Gerätekontrolle
- Verwaltung vor Ort

Zusätzliche Absicherungsverfahren sind nötig für den Schutz mobiler Systeme, wenn diese vom Netzwerk getrennt sind und auch, wenn sie später wieder angeschlossen werden:

- Desktop-Firewall
- Inhaltsfilterung
- Website-Blockierung
- Desktop Host Intrusion Prevention
- Richtlinienkontrolle
- Netzwerkzugriffssteuerung

Eine effektive End Point Protection bietet elementaren E-Mail- und Web-Schutz. Auch mobile Mitarbeiter werden auf diese Weise

Darauf sollten kleine und mittelständische Betriebe achten

- Schutz in Echtzeit, um präventiv auf die ständig wechselnden Bedrohungen einzugehen.
- Auswahl nach Lieferanten und Herstellern, die den Prozess des Sicherheitsmanagements effektiv gestalten können, um die Zeit für manuelle Arbeit zu reduzieren.
- Entwicklung interner Regeln und Herangehensweisen, damit sichergestellt ist, dass jeder mögliche Einfalls- und Angriffspunkt geschützt wird.
- Ausschau nach mehrschichtigen Sicherheitslösungen, wie zum Beispiel die Kombination aus AV-Schutz mit Datenverschlüsselung, damit nicht jede Bedrohung mit unterschiedlichen Produkten behandelt werden muss.
- Security-as-a-Service kann eine sinnvolle Alternative sein. Outsourcing ist vor allem für kleinere Unternehmen eine hervorragende Möglichkeit, IT-Know-how einzukaufen und Wartungskosten auszulagern.

Wichtige Sicherheitsfunktionen beim Endgeräteschutz			
	Kleine Unternehmen	Mittlere Unternehmen	Große Unternehmen
Anti-Virus	Sehr wichtig	Sehr wichtig	Sehr wichtig
Spyware-Schutz	Sehr wichtig	Sehr wichtig	Sehr wichtig
Sicheres Surfen	Sehr wichtig	Sehr wichtig	Sehr wichtig
Anti-Spam	Sehr wichtig	Sehr wichtig	Sehr wichtig
Gerätekontrolle	Sehr wichtig	Sehr wichtig	Sehr wichtig
Verwaltung vor Ort	Sehr wichtig	Sehr wichtig	Sehr wichtig
Desktop-Firewall	Wichtig	Sehr wichtig	Sehr wichtig
Inhaltsfilter	Wichtig	Wichtig	Sehr wichtig
Websites blockieren	Wichtig	Wichtig	Sehr wichtig
Desktop Host Intrusion Prevention	Wichtig	Wichtig	Sehr wichtig
Richtlinienkontrolle	Wichtig	Wichtig	Sehr wichtig
Netzwerkzugriffs-steuerung	Wichtig	Wichtig	Sehr wichtig

präventiv vor Malware und Zero-Day-Bedrohungen geschützt. Die Verwaltung der Lösung sollte möglichst über eine zentrale Konsole stattfinden, die die Einhaltung möglicher Richtlinien und die Zugriffskontrolle steuert. Der zusätzliche Einsatz von Host Intrusion Prevention blockiert ungewünschte Aktivitäten, indem Signaturen, das Verhalten im Netz und die Systeme selbst analysiert werden. Wünschenswert ist außerdem, dass sichergestellt ist, dass nur vertrauenswürdige Anwendungen auf Servern und Endgeräten zur Ausführung kommen. Dies erfolgt bestenfalls über Application Control-Produkte. Wichtig ist, dass solche Lösungen angesichts der immer vielfältigeren Betriebssysteme-Landschaft gerade im Tablet-Bereich zumindest eine effektive Zugangskontrolle für verschiedene Lösungen anbieten.

Schutz der E-Mailumgebung

Viren und Würmer können sich auch über die internen E-Mail-Systeme verbreiten. Eine Security-Lösung für E-Mailserver schützt Sie vor diesen Bedrohungen, blockiert Spam und filtert Nachrichten, die unerwünschte Inhalte enthalten. Absicherungskomponenten zum Schutz von E-Mailsystemen sollten unter anderem Elemente zur Abwehr von Viren und Spam, eine Inhaltsfilterung sowie die Filterung von Anhängen und ausgehender E-Mailnachrichten beinhalten.

E-Mail-Filter leisten Schwerarbeit, denn sie dienen dazu, Viren, Malware, Phishing, Denial-of-Service- und Bounceback-Angriffe abzuwehren. Außerdem müssen sie sorgfältiger und skalierter als je zuvor Spam-Filterung betreiben. Hier stehen für den Mittelstand unterschiedliche Lösungen zur Verfügung. Sie reichen von der Integration von E-Mail-Security-Appliances bis zu Security-as-a-Service-Angeboten, die E-Mails aus der Ferne durchforsten. Die Entscheidung entweder für eine Appliance oder das SaaS-Angebot hängt von möglichen Ressourcen, von den Ansprüchen an die Skalierbarkeit und letztendlich auch von anfallenden Kosten ab.

Schranken für das Extranet

Web-Gateways oder Web-Schutz als Security-as-a-Service filtern das Web auf mögliche Bedrohungen und überprüfen den Inhalt von Webseiten auf Böswilligkeit. Eine optimale Lösung kann über Appliances, in virtuellen Umgebungen oder "in the cloud" implementiert werden. Auch dieses Produkt gibt es als Service.

Fazit

Für alle geschäftlichen Aktivitäten eines mittelständischen Unternehmens muss die IT-Abteilung Prozesse und Regeln erstellen, die in Zeiten von Cloud und Web 2.0 eine adäquate Sicherheitsarchitektur beiseite stellen. Zudem müssen Mitarbeiter, Partner und Kunden geschult werden. Der Spagat, umfassende Sicherheitsanforderungen und begrenzte Ressourcen in Einklang zu bringen, ist eine Herausforderung und ein anspruchsvoller Balanceakt. *(ln)*

Isabell Unseld ist Senior Manager PR bei McAfee.

Wichtige Sicherheitsfunktionen zum Schutz von E-Mailsystemen			
	Kleine Unternehmen	Mittlere Unternehmen	Große Unternehmen
Anti-Virus	Sehr wichtig	Sehr wichtig	Sehr wichtig
Anti-Spam	Sehr wichtig	Sehr wichtig	Sehr wichtig
Inhaltsfilter	Sehr wichtig	Sehr wichtig	Sehr wichtig
Filterung von Anhängen	Sehr wichtig	Sehr wichtig	Sehr wichtig
Filterung ausgehender Email Nachrichten	Sehr wichtig	Sehr wichtig	Sehr wichtig

Wichtige Sicherheitsfunktionen zum Schutz vor Bedrohungen aus dem Internet			
	Kleine Unternehmen	Mittlere Unternehmen	Große Unternehmen
Verhinderung von Netzwerk-Eindringungsversuchen	Sehr wichtig	Sehr wichtig	Sehr wichtig
Web-Filterung	Sehr wichtig	Sehr wichtig	Sehr wichtig
Virenschutz	Sehr wichtig	Sehr wichtig	Sehr wichtig
IP-Reputation	Sehr wichtig	Sehr wichtig	Sehr wichtig
Geolocation-Filterung	Wichtig	Wichtig	Sehr wichtig
Malware-Schutz	Sehr wichtig	Sehr wichtig	Sehr wichtig

Sicherheitsvorfälle im Active Directory erkennen (1)

Rechtzeitige Gefahrenmeldung

von Thomas Gronenwald

Das Active Directory bildet das Herzstück jeder IT-Infrastruktur. Probleme und Schwachstellen innerhalb des Verzeichnisdienstes bedeuten daher schnell ungeplante Ausfälle. Nur durch eine gezielte Überwachung des Verzeichnisdienstes lassen sich mögliche Sicherheitslücken, Verstöße gegen die geltenden Sicherheitsrichtlinien oder gar Angriffe durch Außen- und Innentäter entdecken und geeignete Gegenmaßnahmen einleiten. Die erste Anlaufstelle, nicht nur zur Überwachung, sondern auch als ersten Ansatzpunkt bei der Fehlerdiagnose, stellt dabei das Ereignisprotokoll eines jeden Windows-Betriebssystems dar. Worauf Sie achten müssen und welche Neuerungen Windows Server 2008 R2 dabei mitbringt, erfahren Sie im ersten Teil unserer Workshopserie.

Seit der Einführung von Windows NT war das Ereignisprotokoll oft eine Quelle der Verwirrung und Enttäuschung für Systemadministratoren. Das Ereignisprotokoll enthielt zwar viele Informationen über Sicherheits-, System- oder Benutzerereignisse, diese ließen sich jedoch aufgrund nicht fein genug konfigurierbarer Überwachungsrichtlinien schlichtweg nicht effektiv genug nutzen. Es wurden zwar unzählige Einträge generiert, jedoch enthielten diese in den wenigsten Fällen auch brauchbare Informationen.

Grundlegend neues Auditing mit Windows Server 2008 R2

Mit Windows Server 2008 R2 hat Microsoft das Überwachungssystem grundlegend erneuert und in einigen Punkten stark verbessert, so dass es für Systemadministratoren wesentlich einfacher geworden ist, das Ereignisprotokoll zu kontrollieren und auszuwerten. Leistungs- und Skalierungsprobleme wurden ebenso beseitigt wie die effektive Protokollgröße. Wo beim alten Ereignisprotokolldienst die zu geringe Protokolldateigröße bei maximal 4 GByte lag, können Protokolle unter Windows Server 2008 R2 nun über 1 PByte groß sein. Ebenso konnte das alte Protokoll auch nicht beim Durchsatz überzeugen. Lediglich ein maximaler Durchsatz von wenigen Tausend Ereignissen pro Sekunde war möglich. Das neue Protokoll kann hingegen Zehntausende von Ereignissen pro Sekunde verarbeiten.

Des Weiteren hat Microsoft Änderungen im Bereich der Event-IDs vorgenommen – die Sicherheitsereignisse wurden neu nummeriert und umstrukturiert. Sollten Sie viele Nummern von Sicherheitsereignissen unter Windows Server 2003 auswendig kennen, ist dieses Wissen nicht nutzlos geworden. Generell wurde die Ereignis-ID eines Sicherheitsereignisses in Windows Server 2008 R2 nur um den Wert 4.096 erhöht. So trägt das Ereignis einer erfolgreichen Anmeldung (ID 528 in Windows Server 2003) nun die Ereignis-Nummer 4.624 in Windows Server 2008 R2 (528 + 4.096 = 4.624).

Standardmäßig wird innerhalb des Active Directory bereits eine Vielzahl an Ereignissen überwacht, in den wenigsten Fällen reichen diese jedoch aus, um genaue Rückschlüsse ziehen zu können. Das Active Directory unter Windows Server 2008 R2 stellt insgesamt neun verschiedene Kategorien zur Überwachung bereit – in der erweiterten Überwachungsrichtlinie sogar 53; mehr dazu im Teil 2 dieser Workshopserie. Daher ist es nicht nur wichtig zu wissen, was alles überwacht werden kann, sondern wie es richtig konfiguriert wird.

Das Ereignisprotokoll verstehen

Wie bereits angedeutet, kann das Ereignisprotokoll verwirrend sein – denn nicht jeder Fehler ist auch immer als Fehler einzustufen. Daher ist es ratsam sich mit den täglichen Ereignissen des Betriebes vertraut zu machen – nur so sind Sie auch in der Lage, verschiedene Fehler und vermeidliche Angriffe zeitnah zu erkennen und zu bewerten. Standardmäßig verzeichnet das Ereignisprotokoll fünf Typen von Ereignissen. Dabei werden diese durch unterschiedliche Symbole oder Icons dargestellt:

- Fehler: Symbolisiert durch ein Ausrufezeichen in einem roten Kreis, signalisiert er in der Regel wirkliche Probleme. Typische Beispiele für Fehler sind Dienste, die gestoppt oder angehalten wurden, nicht ordnungsgemäß funktionieren oder beim Systemstart nicht begonnen werden konnten.

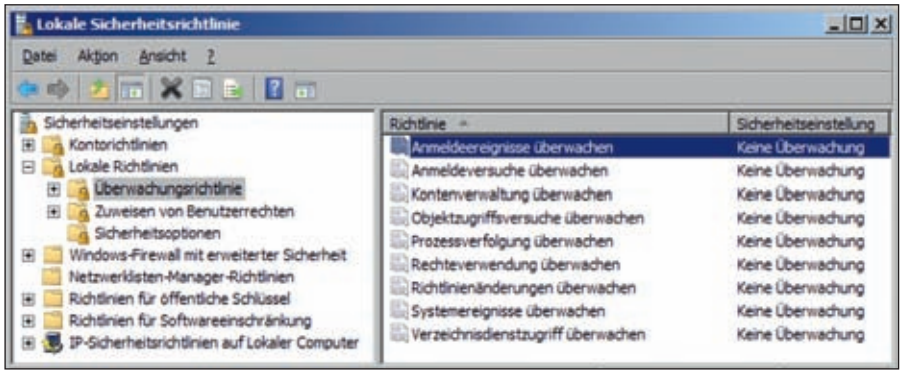


Bild 1: Die Überwachungsrichtlinien erlauben unter anderem das Überwachen von Anmeldeereignissen und Systemereignissen

- Warnungen: Visualisiert durch ein Ausrufezeichen in einem gelben Dreieck, spiegelt eine Warnung Ereignisse wider, die in der Regel den Betrieb nicht beeinflussen, jedoch beobachtet und behoben werden sollten. Typische Beispiele hierfür sind unter anderem zu wenig Speicherplatz oder Abweichungen bei der Synchronisierung der Uhrzeit.
- Informationen: Durch ein "I" in einem weißen Kreis dargestellt, signalisiert dieses Ereignis zumeist, dass eine Aufgabe oder Vorgang erfolgreich abgeschlossen wurde. Ein Informationsereignis wird beispielsweise generiert, wenn ein Dienst erfolgreich gestartet wurde.
- Erfolgsüberwachungen: Als wichtige Bestandteile der Überwachung gelten Erfolgs- und Fehlversuchsüberwachungen. Erfolgsüberwachungen werden als Schlüssel dargestellt. Typische Erfolgsüberwachungen sind beispielsweise erfolgreiche Anmeldungen am Verzeichnisdienst.
- Fehlversuchsüberwachungen: Mit einem Schloss dargestellt werden hingegen Fehlversuchsüberwachungen protokolliert. Typisch hierfür sind Benutzer, die vergeblich versuchen, sich an einem System anzumelden. Hierbei wird dann ein Fehlversuchsüberwachungs-Ereignis generiert.

Arbeit mit Überwachungsrichtlinien

Wie bereits erwähnt, gibt es im Active Directory unter Windows Server 2008 R2 neun beziehungsweise 53 verschiedene Kategorien zur Überwachung. Standardmäßig werden bereits einige davon genutzt – wichtige und für den Administrator interessante Richtlinien sind jedoch zum Teil ausgeschaltet. Damit Ereignisse durch diese Richtlinien innerhalb des Ereignisprotokolls erfasst werden, gilt es, entsprechende Richtlinien zu konfigurieren. Im weiteren Verlauf wollen wir die wichtigsten Richtlinien und Ereignisse einmal genauer betrachten.

Insgesamt stehen neun Überwachungsrichtlinien zur Verfügung. Sieben davon sind sowohl für Clients, Mitgliedsserver als auch für Domänencontroller nutzbar. Zwei der neun Richtlinien sind ausschließlich für die Überwachung von Domänencontroller gedacht und zeigen keine Wirkung, wenn diese auch für Clients und Server konfiguriert werden. Die Überwachungsrichtlinien in der Tabelle "Überwachungsrichtlinien" gehören zu den sieben standardmäßig vorhandenen Kategorien, die sowohl für Clients, Mitgliedsserver als auch für Domänencontroller gelten.

In einigen Szenarien kann es von großem Interesse sein, bestimmte Zugriffe auf verschiedenste Objekte zu überwachen. Über die Objektzugriffsüberwachung kontrollieren Sie etwa innerhalb des Verzeichnisdienstes zu jeder Zeit den erfolgreichen oder fehlgeschlagenen Zugriff auf Objekte wie Freigaben oder Ordner. Das Aktivieren der Überwachung eines Objektes, wie zum Beispiel einer Datei, eines Ordners oder eines Druckers, besteht dabei aus zwei Schritten. Nach der Aktivierung der Überwachungsrichtlinie müssen Sie die SACLs (System Access Control List) der entsprechenden Objekte anpassen. Eine SACL definiert eine Liste von Benutzern und Gruppen, für die Aktionen überwacht werden. Die Aktivierung dieser Einstellung kann auf Domänencontrollern eine große Zahl an Einträgen produzieren. Sie sollten daher nur das überwachen, was Sie wirklich benötigen. Möchten Sie zum Beispiel die Zugriffsversuche der Benutzer auf eine bestimmte Datei überwachen, müssen Sie die entsprechenden Attribute über die Sicherheitseinstellungen der Datei bearbeiten. Wichtige Voraussetzung an dieser Stelle ist, dass für eine Überwachung zwingend das NTFS-Dateisystem genutzt werden muss.

Anmeldeereignisse überwachen

Durch diese Richtlinie legen Sie fest, ob An- und Abmeldungen lokal überwacht werden. Auch hier können Sie sowohl die erfolgreichen als auch die fehlgeschlagenen Anmeldeereignisse überwachen. Definieren Sie die Überwachung auf einem Domänencontroller, wird für Benutzer, die sich an einer Arbeitsstation anmelden, kein Eintrag erzeugt. Nur interaktive Anmeldungen am Domänencontroller beispielsweise durch einen Administrator und Netzwerkanmeldungen generieren ein entsprechendes Ereignis.

Überwachungsrichtlinien im Active Directory

Überwachungsrichtlinie	Standardeinstellung
Objektzugriffsversuche überwachen	Keine Überwachung
Anmeldeereignisse überwachen	Erfolgreiche Ereignisse werden überwacht
Kontenverwaltung überwachen	Erfolgreiche Ereignisse werden überwacht
Systemereignisse überwachen	Erfolgreiche Ereignisse werden überwacht (nur auf Domain Controller), keine Überwachung auf Mitgliedsservern
Rechteverwendung überwachen	Keine Überwachung
Richtlinienänderungen überwachen	Erfolgreiche Ereignisse werden überwacht (nur auf Domain Controller), keine Überwachung auf Mitgliedsservern
Prozessnachverfolgung überwachen	Keine Überwachung
Anmeldeversuche überwachen	Erfolgreiche Ereignisse werden überwacht (nur auf Domain Controller)
Verzeichnisdienstzugriff überwachen	Erfolgreiche Ereignisse werden überwacht (nur auf Domain Controller)

Anmeldeversuche überwachen

Diese Richtlinieneinstellung legt fest, ob die An- und Abmeldeversuche überwacht werden. Sie haben die Möglichkeit, sowohl die erfolgreichen wie auch die fehlgeschlagenen Versuche zu überwachen. Haben Sie die Überwachung auf einem Domänencontroller definiert, wird auch bei dieser Richtlinie für jeden Benutzer, der gegen diesen eine Authentifizierung durchführt, ein Eintrag erzeugt. Dies passiert auch dann, wenn der Benutzer in diesem Moment an einer Arbeitsstation angemeldet ist, die Mitglied der Domäne ist.

Anmeldeversuche vs. Anmeldeereignisse

Die beiden Überwachungsrichtlinien "Anmeldeversuche-" und "Anmeldeereignisse überwachen" verwirren oft aufgrund ihrer ähnlichen Namensgebung und Beschreibungen. Daher ist es an dieser Stelle wichtig, anhand eines einfachen Beispiels Licht ins Dunkel zu bringen. Beispiel: Ein Benutzer meldet sich mit seinem Domänenkonto an einem Client an. Hierbei generiert der Client ein Anmeldeereignis, wohingegen der Domänencontroller einen Anmeldeversuch protokolliert. Identisch verhält es sich auch, wenn auf eine Netzwerkressource zugegriffen wird. Wird beispielsweise eine Freigabe auf einem Fileserver geöffnet, generiert der Fileserver ein Anmeldeereignis, wohingegen der Domänencontroller wiederum einen Anmeldeversuch protokolliert.

Halten wir fest: Aktivieren Sie die Überwachungsrichtlinie für Anmeldeereignisse auf allen Systemen in Ihrer Domäne, werden die Anmeldeereignisse nur auf dem lokalen System selbst (Client, Memberserver oder Domänencontroller) protokolliert. Bei der Überwachungsrichtlinie für Anmeldeversuche hingegen werden die entsprechenden Ereignisse, auch wenn Sie diese für Clients aktivieren, nur auf dem Domänencontroller protokolliert. Daher an dieser Stelle nochmals der Hinweis, dass die Überwachungsrichtlinie für Anmeldeversuche nur auf Domänencontrollern greift.

Kontenverwaltung überwachen

Mit der Überwachung der Kontenverwaltung legen Sie fest, ob auf einem Computer die Verwaltung von Konten überwacht wird. Beispiele für die Kontenverwaltung sind hierbei:

1. Ein Benutzerkonto oder eine Gruppe wird erstellt, geändert oder gelöscht.
2. Ein Benutzerkonto wird umbenannt, deaktiviert oder aktiviert.
3. Ein Passwort wird gesetzt oder geändert.

Auch an dieser Stelle können Sie natürlich wieder eine Erfolgs- oder Fehlerüberwachung konfigurieren. Eine Erfolgsüberwachung ist hierbei auf allen Computern des Unternehmens zu empfehlen. Um Sicherheitsvorfälle zu erkennen, ist es zwingend notwendig, dass Sie feststellen können, wer ein Konto erstellt, geändert oder gelöscht hat.

Systemereignisse überwachen

Die Überwachung von Systemereignissen gehört zu den wichtigsten Komponenten. Sie erzeugt unter anderem Einträge, wenn ein Benutzer versucht ein System neu zu starten oder herunterzufahren. Da die generierten Einträge der Erfolgs- und Fehlerüberwachung sehr wichtig sind, empfiehlt es sich, die Einstellung auf allen Computern Ihrer Organisation zu aktivieren. Die Richtlinie "Rechteverwendung überwachen" legt dabei fest, ob die Verwendung von Benutzerrechten überwacht wird. Bei einer Aktivierung dieser Einstellungen wird eine große Zahl von Einträgen erzeugt. Sie sollten dies daher nur vornehmen, wenn Sie diese Informationen benötigen.

Über "Richtlinienänderungen überwachen" bestimmen Sie, welche Änderungen an Benutzerrechten und Überwachungsrichtlinien protokolliert werden sollen. Die Einstellung "Prozessnachverfolgung überwachen" legt fest, ob detaillierte Aktionen, wie zum Beispiel die Aktivierung von Programmen oder das Beenden von Prozessen, überwacht werden. Auch hier wird eine große Anzahl von Einträgen erzeugt. Sie sollten dies daher nur einrichten, wenn Sie solche Informationen benötigen. Bei einem Sicherheitsvorfall können die Informationen allerdings von großem Nutzen sein. Sie können dann zum Beispiel feststellen, welche Prozesse wann und wie gestartet wurden.

Fehler und Neustarts überwachen

Fehlgeschlagene Aktionen oder Ereignisse repräsentieren keine aktuellen Veränderungen. Trotzdem ist eine Überwachung in den meisten Fällen sinnvoll. Der wesentliche Vorteil hierbei ist, dass beispielsweise fehlerhafte Anmeldungen auf einen Sicherheitsvorfall hindeuten können. In den meisten Fällen werden hier zwar Ereignisse protokolliert, die darauf hinweisen, dass ein Benutzer nicht ausreichende Berechtigungen besitzt, um seinen täglichen Aufgaben nachzukommen, aber es werden auch Hinweise auf mögliche Angreifer geliefert. Daher gilt es an dieser Stelle, geeignete Echtzeitfilter einzusetzen, um Sicherheitsvorfälle schnell und effektiv identifizieren zu können – so sollten Brute-Force-Attacken schnell erkannt werden und somit der Vergangenheit angehören.

Jedes Mal, wenn ein System heruntergefahren oder neugestartet wird, ist es einem nicht unerheblichen Risiko ausgesetzt. Überwachungsmechanismen werden vom Betriebssystem gesteuert, daher gibt es für diesen Zeitraum auch keine Einträge im Ereignisprotokoll. Ein Angreifer hat so die Möglichkeit, unbemerkt Änderungen vorzunehmen und so das System zu manipulieren. Typische Beispiele hierfür sind das Booten von USB oder DVD mit einem eigenen Betriebssystem – der Angreifer hätte so in den meisten Fällen ungehindert Zugriff auf lokale Ressourcen. Natürlich soll das nicht heißen, dass das größte Sicherheitsrisiko ein Neustart ist und dahinter immer ein Angriff steckt. Jedoch sollten Sie diese entsprechend kritisch überwachen und dokumentieren.

Fazit

Bei der Ereignisüberwachung hat sich mit Windows Server 2008 R2 eine Menge getan und zum Positiven gewendet. Im ersten Teil unseres Workshops haben wir einen Blick auf Änderungen in 2008 R2 und die grundlegenden Möglichkeiten bei der Überwachung geworfen. Im zweiten Teil unserer Workshopserie betrachten wir die Konfiguration geeigneter Überwachungsrichtlinien und die wichtigsten Event-IDs. *(dr)*

Bestellen Sie jetzt

das IT-Administrator

Sonderheft 1/2012!

180 Seiten Praxis-Know-how rund um das Thema

Exchange 2010

Migration, Betrieb und Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft I/2012 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.*

Liefertermin:
Ende März 2012

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/2012 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft I/2012 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 1211

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

Penetrationstest mit BackTrack 5

Erlaubtes Eindringen

von Dr. Holger Reibold


Quelle: Pixelio.de

Sicherheitsprodukte haben Hochkonjunktur – auch solche aus dem Open Source-Umfeld, denn sie bieten oftmals eine den kommerziellen Lösungen vergleichbare Funktionalität. Ein Musterbeispiel hierfür ist BackTrack, eine Linux-Distribution, die der Durchführung von Penetrationstests und dem Sammeln von sicherheitsrelevanten Informationen dient. BackTrack gilt als eine Art Schweizer Hacker-Taschenmesser, das auf das Aufspüren von Sicherheitslücken und die Überprüfung der Sicherheit einzelner Rechner in Netzwerken spezialisiert ist. Das Besondere: In dem Testsystem sind alle wichtigen Tools vereint und Sicherheitsbeauftragte können ohne großen Aufwand Sicherheitsanalysen durchführen. Dieser Workshop zeigt die Konfiguration von BackTrack und den Einsatz der Scanner sowie der Schwachstellenwerkzeuge.

Penetrationstests haftet immer auch etwas Negatives an, denn die meisten IT-Verantwortlichen verbinden damit ein Vorgehen, das Zielsysteme derart unter Beschuss nimmt, dass diese im ungünstigsten Fall lahmgelegt werden. Doch das ist in der Regel weder gewünscht noch vorgesehen. Bei Penetrationstests werden jedoch zielgerichtete Attacken mit den Mitteln der Hacker simuliert.

Da die meisten Hacker bei ihren Attacken ebenfalls auf Penetrations-Werkzeuge setzen, genießen diese Sicherheitstools nicht gerade den besten Ruf. Dass Hacker zu Penetrations-Tools statt zu Security-Scanner greifen, hat einen einfachen Grund: Security-Scanner hinterlassen zum Teil erhebliche Einträge in Logfiles beziehungsweise werden schnell von Intrusion Detection-Systemen identifiziert. Die Scanner sind in der Regel auch deutlich langsamer und unterziehen das Zielsystem – je nach Konfiguration – einer sehr intensiven Analyse. Mithilfe eines Penetrationstests versucht der Anwender also mit den Mitteln eines Angreifers, meist auch innerhalb einer gegebenen Zeitspanne, die kritischen Lücken in der IT-Infrastruktur zu identifizieren.

Merkmale und Ziele von Penetrationstests

Das Ziel eines Penetrationstests ist es immer, unautorisiert in die Zielsysteme einzudringen. Der Test versucht sich also nicht nur am Knacken bestehender Sicherheitsmechanismen, sondern liefert Ihnen als Ergebnis immer auch, wie empfindlich das zu testende System gegen derartige Angriffe ist. Ein wesentliches Merkmal der Penetrationstests ist, möglichst viele Angriffsmuster nachzubilden, die sich aus bekannten Angriffsmethoden ableiten. Die Tests berücksichtigen das Gefahrenpotential der verschiedenen zu prüfenden Applikationen und Services. Demnach besitzt ein Webserver eine deutlich höhere Gefahrenpriorität als eine einfache Textverarbeitung.

Um möglichen Missverständnissen vorzubeugen, ist in diesem Zusammenhang auch die Abgrenzung von Penetrationstests zu Vulnerability Scans sinnvoll. Letztgenannte suchen zwar auch nach Sicherheitslücken, doch laufen sie überwiegend automatisch ab. Das ist bei Penetrationstests meist anders, denn die bedürfen der manuellen Vorbereitung, der konkreten Planung und Auswahl der zu verwendenden Testverfahren, der Wahl der notwendigen Werkzeuge sowie der praktischen Durchführung. Da auch der Begriff der Security Scans gefallen ist, auch hierzu noch die Abgrenzung. Sie unterscheiden sich von den Schwachstellen-Scans durch die manuelle Verifizierung der Testergebnisse.

Im Allgemeinen werden Penetrationstests als empirischer Teil einer allgemeineren Sicherheitsanalyse gesehen. In der Praxis vermischen sich die verschiedenen Techniken und Ansätze – das bleibt nicht aus. Dennoch ist wichtig im Hinterkopf zu behalten, dass die Intention und Umsetzung unterschiedlicher Natur sind.

Neuerungen in BackTrack 5

BackTrack gilt als eines der ausgereiftesten Penetrationstest-Werkzeuge, die die Open Source-Familie zu bieten hat. Ein Grund ist die umfassende Ausstattung von BackTrack – doch das alleine wäre nichts Be-

sonderes, denn das Netz ist voll mit freien geeigneten Tools. BackTrack hebt sich schon alleine durch die Tatsache von anderen Programmen ab, dass die Werkzeuge strukturiert sind und in einer benutzerfreundlichen Umgebung ausgeführt werden können, ohne dass der Anwender zuerst staubtrockene Manpages lesen muss.

Inzwischen ist BackTrack in Version 5 verfügbar und genügt dank der umfassenden Ausstattung inzwischen auch den Ansprüchen von professionellen Sicherheitsspezialisten. Gegenüber BackTrack 4 wurde das System beispielsweise um Armitage erweitert, das der Steuerung des Exploit-Frameworks Metasploit dient. Mit Armitage steht eine sehr benutzerfreundliche Umgebung zur Verfügung. Eine weitere interessante Neuerung ist der sogenannte Stealth-Modus. In diesem Modus generiert BackTrack kaum Netzwerktraffic – ideal also für die Durchführung von Penetrationstests. Der größte Pluspunkt für eine breite Akzeptanz ist sicherlich, dass die BackTrack-Umgebung auch optisch deutlich aufgemöbelt wurde. Gerade Einsteiger und Neulinge in diesem Bereich werden dies zu schätzen wissen.

Über die BackTrack-Projektseite [1] stehen verschiedene Varianten der Sicherheitsumgebung zum Download bereit. Neben der gewohnten x86-Ausgabe gibt es auch eine 64 Bit-Version. Wenn Sie mit einem 32 Bit-System arbeiten, können Sie BackTrack auch als VMware-Version testen. BackTrack ist außerdem in einer ARM-Version verfügbar, um es beispielsweise auf einem Android-Tablet auszuführen. Je nach Variante sind die DVD-Images zwischen 1 und 1,9 GByte groß.

BackTrack in Betrieb nehmen

Um BackTrack einzusetzen, erzeugen Sie aus dem Download-Image, das zu Ihrer Plattform passt, zunächst eine Boot-CD. Diese startet standardmäßig das BackTrack-Live-System. Dieses erlaubt anschließend auch die Installation. Für ein erstes Kennenlernen ist die Live-Umgebung sicherlich ausreichend.

Für die Anpassung der Live-CD steht Ihnen ein komfortables Skript [2] zur Verfügung, mit dem Sie einige rudimentäre

Bild 1: BackTrack ist als Live-CD nutzbar und bietet beim Booten Setups für unterschiedliche Einsatzzwecke

Einstellungen anpassen. Sie können etwa das Starten beziehungsweise die gezielte Installation von bestimmten Paketen oder Treibern (beispielsweise WLAN-Treiber) initialisieren und lässt sich sowohl unter BackTrack 4 also auch unter seinen Nachfolgern ausführen.

Wenn Sie die Penetrationsumgebung einer ausführlichen Evaluierung unterziehen wollen, sollten Sie diese auf einem Testsystem installieren. Loggen Sie sich als root mit dem Passwort "toor" in das System ein. Der Zugriff auf die GUI, über die alle Tools der BackTrack-Umgebung verfügbar sind, erfolgt mit dem Kommando *startx*.

In seltenen Fällen, wenn Sie BackTrack beispielsweise unter VMware ausführen, kann es vorkommen, dass der X-Server nicht vollständig startet. In diesem Fall ist zunächst eine Rekonfiguration des X-Server-Pakets erforderlich. Um einen Reset der Xorg-Konfiguration durchzuführen, verwenden Sie folgenden Befehl:

```
root@bt:~# dpkg-reconfigure
  xserver-xorg
```

Wenn Sie Backtrack 5 auf einem 64 Bit-System mit der KDE einsetzen, sollten Sie den Cache entfernen:

```
root@bt:~# rm /root/.kde/cache-*
```

Sollten die beiden genannten Befehle immer noch nicht die gewünschte Wirkung entfalten, entfernen Sie den Cache-Ordner "/var/tmp" mit folgendem Befehl:

```
root@bt:~# rm -rf /var/tmp/kdecache-*
```

Netzwerk konfigurieren

Vermutlich ist Ihrer Aufmerksamkeit nicht entgangen, dass BackTrack ohne Netzwerkunterstützung gebootet wird. Der Grund hierfür: Die Erhöhung der "Heimlichkeit". Das BackTrack-System wird also nicht so schnell erkannt. Für die Netzwerkkonfiguration können Sie verschiedene Wege einschlagen. Sie können dem BackTrack-System die IP-Adresse manuell zuteilen, diese per DHCP zuweisen, das Networking-Skript oder auch den Wicd Network Manager verwenden. Nehmen wir an, Sie wollen folgende Zielkonfiguration realisieren:

- IP-Adresse: 192.168.1.100/24
- Standard-Gateway: 192.168.1.1
- DNS-Server: 192.168.1.1

Um diese Konfiguration für das BackTrack-System zu realisieren, verwenden Sie folgende Kommandos:

```
root@bt:~# ifconfig eth0
  192.168.1.100/24
root@bt:~# route add default gw
  192.168.1.1
root@bt:~# echo nameserver
  192.168.1.1 > /etc/resolv.conf
```

Das Beziehen der IP-Adresse über einen DHCP-Server lässt sich einfach mit dem Befehl *dhclient {interface}* konfigurieren:

```
root@bt:~# dhclient eth0
[…]
Listening on
  LPF/eth0/00:03:0d:60:fd:ce
Sending on
  LPF/eth0/00:03:0d:60:fd:ce
Sending on   Socket/fallback
DHCPREQUEST of 192.168.1.100 on eth0
  to 255.255.255.255 port 67
DHCPACK of 192.168.1.100 from
  192.168.1.1
bound to 192.168.1.100 – renewal in
  329395 seconds
```

Alternativ verwenden Sie das networking-Skript des Verzeichnisses "/etc/init.d", das dafür sorgt, dass alle Netzwerkschnittstellen, die in "/etc/network/interfaces" angelegt sind, gestartet werden. Sie rufen das Skript mit dem Befehl

```
root@bt:~# /etc/init.d/networking
  start
```

auf. Eine weitere Möglichkeit, um die Netzwerkfunktionalität von BackTrack zu aktivieren: Greifen Sie zum Wicd, der über das Menü "Internet / Wicd Network Manager" verfügbar ist. Womöglich wird beim Starten des Tools eine Fehlermeldung ausgegeben, dass keine Verbindungsaufnahme zum Bus-Interface des Netzwerkmanagers möglich ist. In diesem Fall hilft nur ein Neustart des BackTrack-Systems. Vor der erneuten Ausführung des Netzwerkmanagers sollten Sie die beiden folgenden Kommandos ausführen:

```
root@bt:~# dpkg-reconfigure wicd
root@bt:~# update-rc.d wicd defaults
```

Nach einem neuerlichen Reboot sollte die Fehlermeldung der Vergangenheit angehören. Es versteht sich von selbst, dass Sie das unsichere Root-Passwort mit *passwd* ändern.

Als Nächstes sollten Sie verschiedene Services starten, auf die BackTrack zurückgreift. Dazu gehören beispielsweise Apache, SSH, MySQL und VNC. Hierfür verwenden Sie die Init-Skripts des Linux-Systems. Folgendermaßen starten Sie den SSH-Dienst:

```
root@bt:~# sshd-generate
  # Erzeugt die SSH-Schlüssel
root@bt:~# /etc/init.d/ssh start
Starting OpenBSD Secure Shell
  server: sshd.
```

Damit ein Service beim Booten aktiviert wird, verwenden Sie den Befehl *update-rc.d*. Um SSH immer beim Booten zu starten, nutzen Sie:

```
root@bt:~# update-rc.d -f ssh
  defaults
 Adding system startup for
  /etc/init.d/ssh ...
  /etc/rc0.d/K20ssh -> ../init.d/ssh
  /etc/rc1.d/K20ssh -> ../init.d/ssh
  /etc/rc6.d/K20ssh -> ../init.d/ssh
  /etc/rc2.d/S20ssh -> ../init.d/ssh
  /etc/rc3.d/S20ssh -> ../init.d/ssh
  /etc/rc4.d/S20ssh -> ../init.d/ssh
  /etc/rc5.d/S20ssh -> ../init.d/ssh
```

Damit ist die Grundkonfiguration von BackTrack abgeschlossen. Sie sollten außerdem ein wenig mit den Paketmanagern *apt* und *dpkg* vertraut sein, um gegebenenfalls benötigte Pakete nachzuinstallieren.

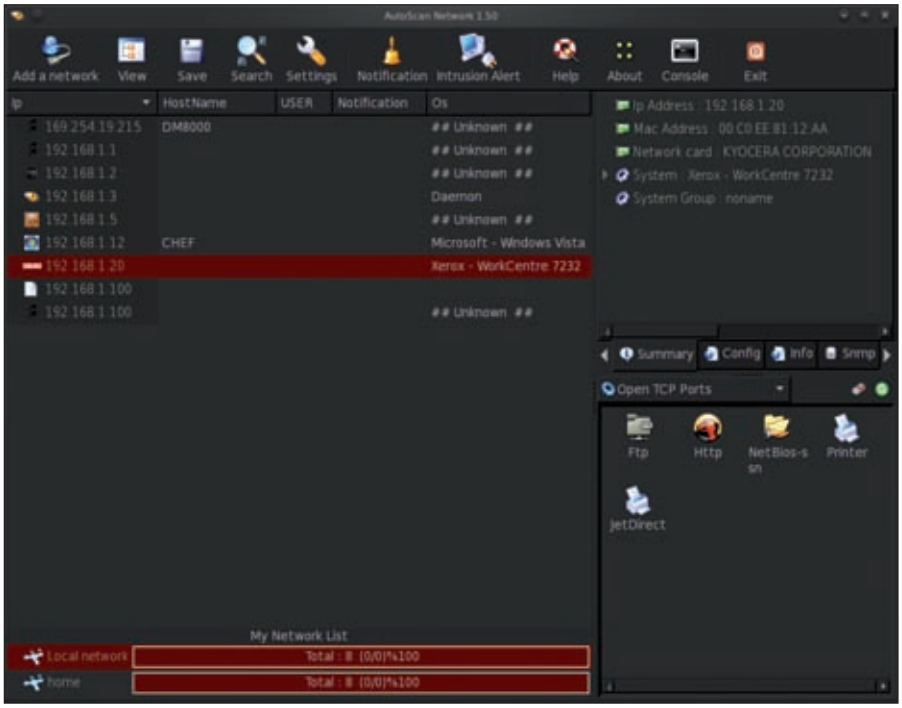


Bild 2: Der Netzwerkscanner "Autoscan" sucht permanent neue Geräte im Netz

Geräte im Netz finden

Die unzähligen Tools, die Ihnen die BackTrack-Umgebung zur Verfügung stellt, stehen über die GUI im Menü "BackTrack" zur Verfügung. Dort finden Sie zwölf Untermenüs, in denen die verschiedenen Tools in Kategorien wie "Information Gathering", "Exploitation Tools", "Forensics" und "Reporting Tools" zusammengefasst sind.

Informationen über die Zielsysteme und deren Schwachstellen sind der Ausgangspunkt für die weitere Analyse und den gezielten Einsatz anderer Tools, die BackTrack bereitstellt. Wenn Sie einen ersten Blick in das Untermenü "Information Gathering" werfen, werden Sie nicht schlecht stauen: Dieses umfasst zwei weitere Untermenüs mit Dutzenden weiterer Werkzeuge.

Eines der interessantesten Werkzeuge ist "Autoscan", das Sie im Untermenü "Network Analysis / Network Scanners" finden. Es handelt sich um einen grafischen Spezialisten für das Erkennen von Netzwerkkomponenten. Seine Hauptaufgabe ist es, Rechner und Netzwerkkomponenten in der Infrastruktur schnell zu identifizieren. Nach dem Start des Tools meldet sich der Konfigurationsassistent, der Sie durch die verschiedenen Einrichtungsschritte führt. Sie müssen zunächst eine erste Netzwerkkonfiguration anlegen. Dazu genügt es, den

Netzwerkadapter und das zu scannende Netzwerk zu bestimmen. Damit ist Autoscan konfiguriert. Das Tool scannt das Netzwerk permanent nach neuen Netzwerkkomponenten. Die Geräteerkennung erfolgt auf Paketbasis. Dabei macht sich Autoscan eine Datenbank mit Fingerabdrücken der gängigsten Geräte zunutze.

Geräte, die Autoscan nicht eindeutig identifizieren kann, landen in einer speziellen Liste. Während Autoscan das Netzwerk durchsucht, werden neue Geräte im linken Dialogbereich aufgeführt. Wenn Sie einen Eintrag markieren, werden rechts zwei weitere Bereiche eingeblendet, denen Sie verschiedene Details entnehmen können: IP-Adresse, MAC-Adresse, Hersteller des Netzwerkadapters und offene Ports. Rechts gibt Autoscan außerdem die Anzahl der gefundenen Geräte und die Anzahl der anstehenden Scans aus.

Auf Verwundbarkeiten scannen

Zum BackTrack-Paket gehören auch einige Tools, mit denen Sie die Zielsysteme auf Verwundbarkeiten hin überprüfen. Die entsprechenden Werkzeuge finden Sie im Menü "Vulnerability Assessment". Wenn Ihr Augenmerk in erster Linie auf der Prüfung von typischen Web-Applikationen liegt, so finden Sie im Untermenü "Web Assessment" über ein Dutzend Spezialisten. Die eigentlichen Security-Scanner finden Sie im Untermenü "Network Assessment / Vulnerability Scanners". Neben Mantra steht dort auch Nessus, allerdings in Version 2.x, zur Verfügung.

Sie können auch den Nessus-Fork OpenVAS in das BackTrack-System integrieren. Dazu müssen Sie allerdings die OpenVAS-Installation nachholen. Führen Sie dazu die beiden folgenden Befehle aus:

```
root@bt:~#apt-get update
root@bt:~#apt-get install openvas
```

Nach der erfolgreichen Installation finden Sie auch OpenVAS in diesem Untermenü. Bevor Sie allerdings OpenVAS aus BackTrack heraus einsetzen können, sind einige weitere Vorarbeiten erforderlich. Zunächst müssen Sie den OpenVAS-Administrator anlegen. Dazu führen Sie den Befehl *OpenVAS Adduser* aus dem OpenVAS-Menü aus. Sie können jeden beliebigen Benutzernamen verwenden, auch root. Der nächste Schritt dient dem Erstellen des Zertifikats. Es wird für die Absicherung der Kommunikation zwischen OpenVAS-Client und -Server verwendet. Dazu führen Sie den Befehl *OpenVAS Mkcert* aus und folgen den Anweisungen im Dialogfenster. Schritt 3 dient dem Abgleich der sogenannten NVTs. Das sind Testskripts, die von den OpenVAS-Entwicklern für die Analyse der Zielsysteme bereitgestellt werden. Den Abgleich starten Sie mit dem NVT Sync-Befehl.

Damit sind die notwendigen Arbeiten für die Ausführung des OpenVAS-Scanners geleistet und Sie können den Scanner das erste Mal starten. Der Ladevorgang kann beim ersten Mal durchaus einige Minuten in Anspruch nehmen, weil die Plug-Ins, also die Testskripts, geladen werden müssen. Der Scanner wird übrigens nach dem Starten so lange im Hintergrund ausgeführt, bis Sie einen Neustart des Systems ausführen oder diesen gezielt anhalten.

Die Steuerung des OpenVAS-Scanners erfolgt über den sogenannten OpenVAS-Manager. Auch der muss eingerichtet werden. Dazu genügt die Ausführung des folgenden Befehls:

```
openvas-mkcert-client -n om -i
```

Die OpenVAS-Datenbank muss noch mit den neuen NVTs aktualisiert werden. Dies erledigen Sie mit *openvasmd --rebuild*. Als Nächstes müssen Sie noch einen administrativen Benutzer anlegen, den sogenannten OpenVAS-Administrator. Er ist für die Durchführung der Tests zuständig. Sie legen diesen mit folgendem Kommando an:

```
openvasad -c 'add_user' -n
  openvasadmin -r Admin
```

Starten Sie dann den OpenVAS-Manager, der als Hintergrund-Daemon läuft mit:

```
openvasmd -p 9390 -a 127.0.0.1
```

Auch der OpenVAS-Administrator muss gestartet werden:

```
openvasad -a 127.0.0.1 -p 9393
```

Das Besondere an OpenVAS ist die webbasierte Steuerzentrale, die die Ausführung und Auswertung der Tests über eine Web-Schnittstelle erlaubt. Dieses Tool starten Sie über:

```
gsad –http-only –listen=127.0.0.1 -p
  9392
```

Alternativ können Sie auch zum Greenbone Security Desktop greifen, einer Desktop-Anwendung, die im BackTrack-

Lesen Sie den IT-Administrator als E-Paper

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

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

Infos zu E-Abos, E-Einzelheften und Kombiangeboten finden Sie auf:
www.it-administrator.de/magazin/epaper

System integriert ist, aber auch für Mac OS X und Windows verfügbar ist.

Schwachstellen und Exploits finden

Im BackTrack-System sind auch verschiedene Tools enthalten, die der Ausführung von Exploits dienen. Das bekannteste ist zweifelsohne das Metasploit Framework. Sie rufen es über das Menü "Exploitation Tools / Network Exploitation Tools / Metasploit Framework" auf. In dem Exploit-Menü finden Sie eine Vielzahl weiterer Tools, auch die Bereiche Web, Datenbank, WLAN und sogar Social Engineering sind abgedeckt. Für die Netzwerkanalyse greifen Sie zum Metasploit Framework, das dank des in BackTrack 5 integrierten Armitage nun auch recht einfach zu handhaben ist.

Die Verwendung des Frameworks ist unkompliziert: Zunächst wählen Sie einen Exploit aus und konfigurieren diesen. Die in BackTrack 5 enthaltene Metasploit-Version 4.0 beinhaltet 716 verschiedene Exploits für Windows, Unix/Linux, Mac OS X und andere Systeme. Gegebenenfalls ist zu prüfen, ob das Zielsystem für den gewählten Exploit überhaupt verwundbar ist. Der nächste Schritt dient der Wahl des Payload, also des Codes, der auf dem Zielrechner bei einem erfolgreichen Einbruch ausgeführt werden soll. Welche weiteren Aktionen nach dem Eindringen anstehen, ist von der Zielsetzung der Attacke abhängig. Das Besondere an Metasploit: Das Framework kann jeden Exploit mit jeder kompatiblen Nutzlast kombinieren.

Wenn Sie Metasploit sehr intensiv nutzen wollen, so bietet es sich an, eine MySQL-Datenbank als Backend für das Metasploit Framework zu verwenden. Dazu sind einige Anpassungen der BackTrack-Standardkonfiguration notwendig. Führen Sie folgende Befehle aus:

```
root@bt:~# apt-get update
root@bt:~# apt-get dist-upgrade
root@bt:~# service mysql start
root@bt:~# msfconsole
```

Der Befehl *db_driver* sollte nun die Verfügbarkeit der MySQL-Option zeigen. Die entsprechende Ausgabe müsste wie folgt aussehen:

```
msf >db_driver
[*] Active Driver: postgresql
[*] Available: postgresql, mysql
```

Damit ist sichergestellt, dass Metasploit MySQL ansprechen kann. Stellen Sie nun aus Metasploit heraus die Verbindung zu MySQL mit dem Passwort "toor" her:

```
msf >db_driver mysql
[*] Using database driver mysql
msf > db_connect
  root:toor@127.0.0.1/msf3
```

Armitage vereinfacht die Verwendung von Metasploit deutlich. Die GUI stellt Ihnen drei Bereiche zur Verfügung: links oben die Modul-Auswahl, rechts oben die Zieldefinition und unterhalb der beiden die verschiedenen Registerkarten. In der Modul-Auswahl bestimmen Sie, welches Exploit ausgeführt werden soll, können den Payload generieren und sogar Skripte für die Ausführungen nach dem Eindringen in das System festlegen. Unterhalb der Auswahl steht Ihnen eine Suchfunktion zur Verfügung, mit der Sie nach dem gewünschten Modul recherchieren können.

Um eine Exploit-Konfiguration zu verwenden, klicken Sie doppelt auf den Eintrag. Sie passen im zugehörigen Dialog verschiedene Exploit-Optionen wie die IP-Adresse, den Port und die zu verwendende Funktion an. Mit einem Klick auf "Launch" führen Sie den Exploit aus.

Der Target-Bereich rechts oben führt alle angelegten Zielsysteme auf. Dazu stehen Ihnen eine grafische und eine tabellarische Darstellung zur Verfügung. Auch aus dem Target-Bereich können Sie mit einem Rechtsklick Scans starten. Unterhalb der Modul- und Zieldefinition präsentiert Ihnen Armitage standardmäßig die Konsole, die Ihnen die Interaktion mit dem attackierten System erlaubt. Bei jeder Exploit-Ausführung wird eine weitere Registerkarte geöffnet, die Ihnen die Eingabe von Kommandos erlaubt.

Umfangreicher Profiwerkzeugkasten

Wollten wir jedes Tool und seine Möglichkeiten beschreiben, das in der BackTrack-Umgebung enthalten ist, so ließe sich damit problemlos ein ganzes Buch füllen. Damit Sie dennoch einen Eindruck gewinnen, wie breit gefächert die Palette an Tools ist, stellen wir Ihnen noch einige Highlights vor.

In der Rubrik "Privilege Escalation" finden Sie eine Fülle an Werkzeugen, mit denen Sie beispielsweise Passwörter knacken können. Dazu gehören auch verschiedene Sniffer. Auch der Klassiker Wireshark gehört zur BackTrack-Grundausstattung. BackTrack besitzt sogar einen ganzen Werkzeugkasten an Reverse Engineering-, RFID- und Stress Testing-Tools.

Besondere Beachtung verdienen die Programme der Untermenüs "Forensics" und "Reporting". In der Forensik-Kategorie finden Sie beispielsweise die Klassiker Autopsy und Sleuthkit. Auch Foremost und Scalpel sind in BackTrack integriert. BackTrack 5 kann sogar im Forensik-Modus gebootet werden. Bei dieser Boot-Variante erfolgt keinerlei Dateisystemzugriff auf das zu analysierende System. Das Untermenü "Services" erlaubt Ihnen außerdem das Starten und Anhalten der wichtigsten BackTrack-Services, beispielsweise des Apache-Servers und des Snort-Dienstes.

Fazit

Mit BackTrack 5 steht Ihnen der mit Abstand ausgereifteste freie Werkzeugkasten für die Durchführung von Penetrationstests und Sicherheits-Audits zur Verfügung. Der Zugriff und die Ausführung der meisten Tools ist inzwischen so einfach, dass diese auch von weniger erfahrenen Anwendern durchgeführt werden können. Einziges Manko ist und bleibt die Dokumentation. Zwar gibt es auf der BackTrack-Website ein kleines Wiki, doch das beschränkt sich leider auf die Beschreibung weniger Grundfunktionen. *(jp)*

Link-Codes

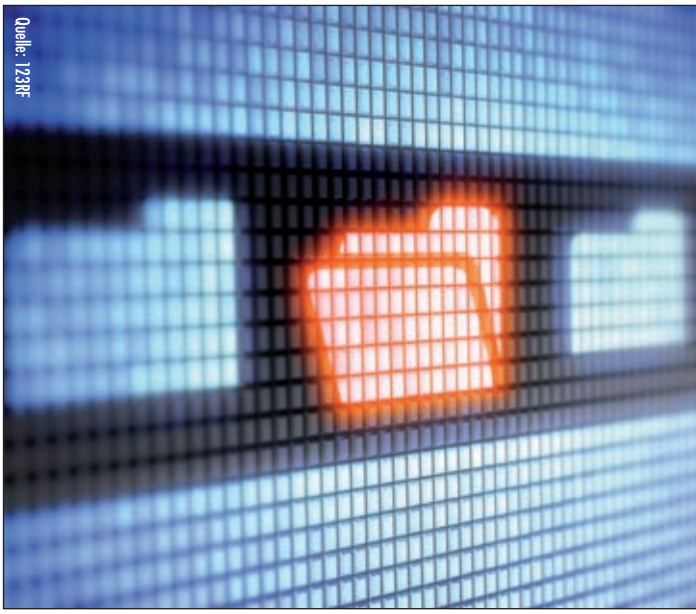
[1] BackTrack-Homepage
BBP21

[2] Skript zur Anpassung der Live-CD
BBP22

Intrusion Detection und -Prevention mit Prelude

Gewusst, wo

von Thorsten Scherf



Security Informations- und Event Management-Systeme dürfen heute in keinem Unternehmen mehr fehlen. Schon alleine die Umsetzung und Einhaltung von Compliance-Vorschriften wie SOX/PCAOB oder PCI/DSS erfordern solche Systeme, wie es das freie Prelude für Linux darstellt. Dank seines modularen Aufbaus ist es extrem flexibel und leicht erweiterbar. Ein übersichtliches Webinterface hilft zudem dabei, den Überblick über die sicherheitsrelevanten Meldungen zu behalten. Lesen Sie, mit welchen Schritten Sie die Prelude einrichten und auf Ihre Bedürfnisse hin feintunen.

Kamen früher getrennte Tools für die Überwachung eines Systems und des Netzwerkverkehrs zum Einsatz – Host-basierte und Netzwerk-basierte Intrusion Detection/Prevention Systems (HIDPS/NIDPS) –, so finden sich diese heutzutage in einer einzelnen Applikation wieder. Jedoch existieren nach wie vor einige Probleme beim Umgang mit solchen Systemen. Zum einen gilt es, den richtigen Schwellenwert zwischen Meldungen zu finden, die einen wirklichen Einbruchsversuch darstellen, und sogenannten False/Positive-Meldungen. Letztere kommen beispielsweise zustande, wenn bestimmte Anwendungen sich nicht an RFCs halten, SIEM-Signaturen aber strikt auf Basis solcher Signaturen arbeiten.

Auch zu strenge Regelsätze können solche Meldungen hervorrufen. Die Folge ist eine Vielzahl von unnötigen Logmeldungen, die das Aufspüren von echten Einbruchsversuchen erschweren können, da der Administrator mit zu vielen Meldungen konfrontiert wird und somit den sprichwörtlichen Wald vor lauter Bäumen nicht mehr sieht.

Zum anderen besteht seit jeher die Schwierigkeit, die generierten Logs in einer Art und Weise aufzubereiten, dass der zuständige Security-Admin diese leicht nach möglichen Problemfällen durchforsten kann.

Sensoren sorgen für Überblick beim Security-Management

Um dem ersten Problem zu begegnen, bietet Prelude [1] eine Vielzahl von Sensoren an – diese sind in der Lage, Logmeldungen aus unterschiedlichsten Quellen miteinander zu korrelieren und somit eine Verbindung zwischen diesen herzustellen. Für diesen Schritt normalisiert Prelude die Meldungen verschiedenster Sub-Systeme in das Intrusion Detection Message Exchange Format (IDMEF) und speichert diese in einer SQL-basierten Datenbank.

Zu diesen Sub-Systemen gehören heterogene Sensoren wie Snort, Samhain, Auditd, NuFw, OSSEC, Nepenthes oder auch diverse Hardware-Geräte wie Cisco-Appliances oder Juniper- und SonicWALL-Firewalls. Jeder dieser Sensoren stellt dem Prelude-Manager Informationen über festgestellte Aktivitäten zur Verfügung – das können lokale Syslogd- oder Auditd-basierte Meldungen, Nachrichten über verdächtige Aktivitäten im IP-Verkehr wie auch Informationen basierend auf einer Windows Registry-Überwachung sein. Sämtliche Informationen fließen dabei über gesicherte SSL-Verbindungen zum zentralen Management-System, dem Prelude-Manager.

Auch die Prelude-Manager selbst können sich untereinander verbinden und Meldungen austauschen, um so ein noch größeres Einzugsgebiet für wichtige Meldungen zu erhalten. Dies ist gerade dann interessant, wenn dedizierte Management-Systeme an geographisch unterschiedlichen Standorten zum Einsatz kommen. Aus all diesen Informationen bildet Prelude ein gemeinsames Bild und stellt es dem Administrator über ein elegantes Webfrontend zur Verfügung. Mit Hilfe jedes gängigen Webbrowers erhält der Admin somit Zugang zu sämtlichen Meldungen. Das Frontend Prewikka stellt diese sehr übersichtlich und grafisch aufbereitet dar. In der kostenpflichtigen Prelude-Pro-Version stehen Features wie grafische Statistiken, PDF-Export oder ein Event-basiertes Ticket-System zur Verfügung.

Die Prelude-Bibliothek, libprelude, besitzt ausserdem eine sehr mächtige API. Mit dieser ist es ohne weiteres möglich, eigene Programme und Skripte an Prelude anzubinden, solange diese in Perl, Python, Ruby, C++ oder einigen weiteren Sprachen vorliegen. Somit wird der bereits sehr mächtige Funktionsumfang von Prelude noch weiter ausgebaut.

Prelude-Manager als Schnittstelle installieren

Als wichtigste Prelude-Komponente ist zuerst der Prelude-Manager zu installieren. Dieser stellt die Schnittstelle zwischen den einzelnen Sensoren und dem Webinterface Prewikka dar. Die Komponenten kom-

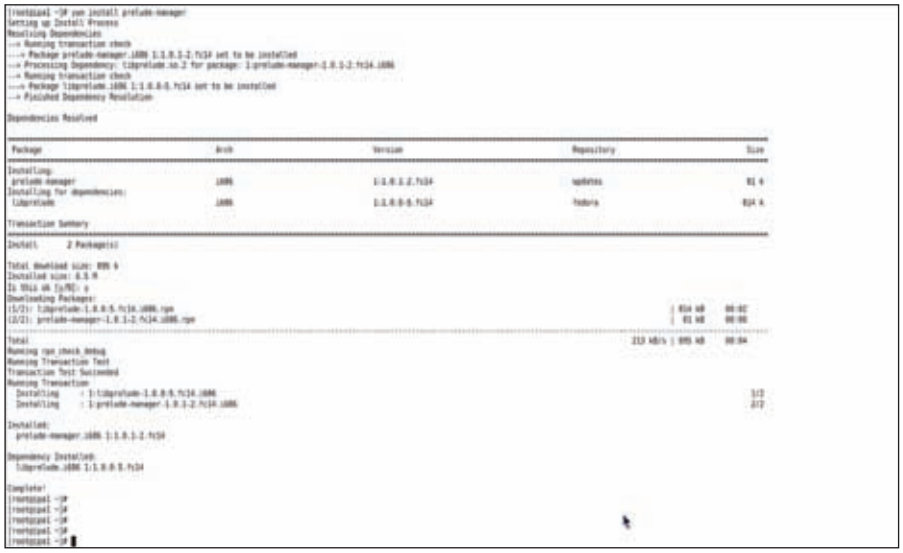


Bild 1: Auf einem Fedora-System gelingt die Installation aller Prelude-Komponenten bequem über das Paket-Management-Tool yum

munizieren dabei über mittels libprelude erzeugte SSL-Verbindungen mit dem zentralen Manager. Dieser Workshop beschreibt das Setup unter einer Fedora 14-Installation, allerdings existieren auch für alle anderen bekannten Linux-Distributionen fertige Installationspakete. Sollte dies einmal nicht der Fall sein, stehen auf der Webseite Archiv-Dateien mit den Quellen der Software zur Verfügung. Über den klassischen Dreisatz *configure*, *make*, *make install* gelingt dann auch eine Installation aus den Quell-Dateien heraus.

Unter Fedora sorgt der Aufruf von *yum install prelude-manager* dafür, dass das Paket aus dem Standard-Repository der Installation geladen und aufgespielt wird. Da das Paket eine Abhängigkeit zu libprelude besitzt, installiert yum dieses Paket direkt mit. Als Nächstes gilt es, die Konfigurationsdatei */etc/prelude-manager/prelude-manager.conf* entsprechend den eigenen Gegebenheiten anzupassen. Hier sind zwei Abschnitte besonders interessant: Zuerst müssen Sie die listen-Anweisung so ändern, dass der Manager nicht nur auf der Loopback-Karte auf eingehende Pakete von den diversen Sensoren wartet, sondern auf der Karte lauscht, die in das richtige Netzwerk zeigt. Ob dies das reguläre Datennetz ist oder ein eigenes Netzwerk nur für die Sensoren existiert, spielt erst einmal keine Rolle. In einem produktiven Umfeld bietet es sich natürlich an, für die Sensoren-Kommunikation ein eigenes VLAN einzurichten. Als Nächstes passen Sie den Datenbank-Abschnitt an. Je nach vorhandener Datenbank tragen Sie hier die passenden Werte ein. Das nachfolgende Listing zeigt ein Beispiel für eine MySQL-Datenbank, die wir auch direkt im nächsten Schritt einrichten:

```
[db]
# Datenbank-Type
type = mysql
# Datenank-Host
host = localhost
# Datenbank-Port
port = 3306
# Datenbank-Name
name = prelude
# Datenbank-Benutzer
user = prelude
# Passwort für den
  Datenbank-Benutzer
pass = redhat
```

Das Setup der eigentlichen Datenbank gelingt auch in wenigen Schritten. Das nächste Listing zeigt den Ablauf. Wichtig ist, dass Sie vor diesen Schritten das Paket *libpreludedb-mysql* installieren. Dies sorgt dafür, dass alle notwendigen Dateien für das MySQL-Setup vorhanden sind. Das Paket besitzt ebenfalls eine Abhängigkeit zum eigentlichen MySQL-Server, so dass yum diesen praktischerweise direkt mit installiert. Da die MySQL-Datenbank nur vom Prelude-Manager erreichbar sein muss, bietet es sich an, die Konfigurationsdatei */etc/my.cnf* um den Eintrag "bind-address=127.0.0.1" zu erweitern. Dies unterbindet Anfragen von externen Rechnern. Voraussetzung hierfür ist natürlich, dass Prelude und der MySQL-Server auf dem gleichen System installiert wurden.

```
# yum install -y libpreludedb-mysql
# mysql -u root
Welcome to the MySQL monitor.
  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.1.58 Source
  distribution
[…]
mysql> CREATE database prelude;

Query OK, 1 row affected (0.01 sec)

mysql> GRANT ALL PRIVILEGES ON
  prelude.* TO prelude@'localhost'
  IDENTIFIED BY 'redhat';

Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye

# mysql -u prelude prelude -p <
  /usr/share/libpreludedb/classic/my
  sql.sql

Enter password:
```

Abschließend richten Sie mittels *prelude-admin add prelude-manager -uid 0 -gid* den Benutzer "prelude-manager" ein und starten mit *service prelude-manager start* schließlich den Dienst.

Mehr Übersicht dank Prewikka

Eine übersichtliche Management-Oberfläche hilft dabei, den Überblick zu bewahren. Prewikka ist ein solches Frontend. Über den Befehl *yum install -y prewikka* gelangt es aus dem Software-Repository der Distribution auf das eigene System. Yum kümmert sich wieder um die Abhängigkeiten, wovon diesmal jede Menge existieren. Da auch Prewikka einer MySQL-Datenbank im Backend bedarf – wer lieber mit SQLite oder PostgreSQL arbeitet, kann natürlich auch diese verwenden –, läuft die Konfiguration ähnlich ab wie beim Prelude-Manager:

```
# yum install -y prewikka
mysql> CREATE database prewikka;
Query OK, 1 row affected (0.00 sec)
```

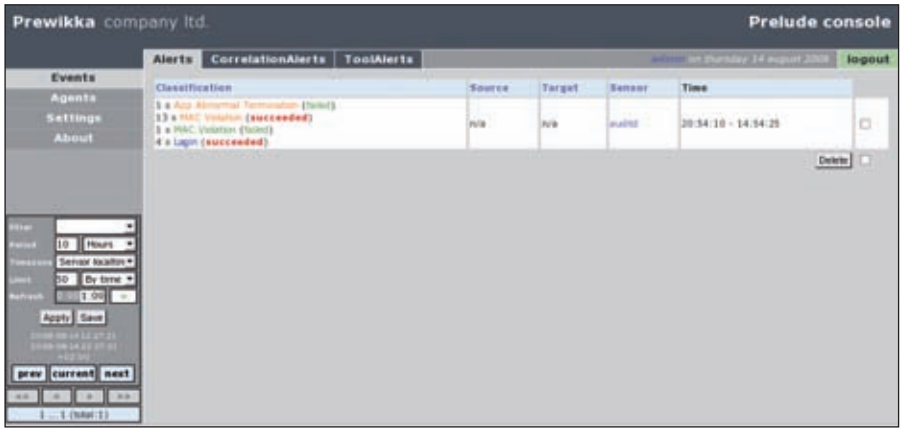


Bild 2: Prewikka kann eine Übersicht aller Event-Klassen anzeigen...

```
mysql> GRANT ALL PRIVILEGES ON
  prewikka.* TO prewikka@'localhost'
  IDENTIFIED BY 'redhat';

Query OK, 0 rows affected (0.00 sec)

mysql> exit

Bye

# mysql -u prewikka prewikka -p <
  /usr/share/prewikka/database/mysql
  .sql

Enter password:
```

In der Datei */etc/prewikka/prewikka.conf* nehmen Sie dann in der entsprechenden Sektion die Angaben zur Datenbank vor. Das Paket bringt einen eigenen Webserver mit. Dieser lässt sich über den Befehl */usr/sbin/prewikka-httpd* starten und steht anschließend auf dem Netzwerkport 8.000 für Anfragen an Prewikka zur Verfügung. Schöner und sicherer ist es natürlich, Prewikka unter Apache oder einem anderen Standalone-Server zu konfigurieren. Das folgende Beispiel richtet Prewikka als virtuellen Host unter einem Apache ein. Hierfür ist natürlich zuerst das Apache-Paket httpd zu installieren. Anschließend ist die Konfigurationsdatei des Webservers */etc/httpd/conf/httpd.conf* um einen Eintrag für einen virtuellen Host zu erweitern. Dieser Abschnitt ist im nachfolgenden Listing beispielhaft dargestellt:

```
<VirtualHost *:80>
 ServerName prewikka.tuxgeek.de
 Setenv PREWIKKA_CONFIG "/etc/
  prewikka/prewikka.conf"
<Location "/">
        AllowOverride None
        Options ExecCGI
        <IfModule mod_mime.c>
                AddHandler cgi-
                script .cgi
        </IfModule>
        Order allow,deny
        Allow from all
</Location>
Alias /prewikka/ /usr/share/
  prewikka/htdocs/
ScriptAlias /prewikka
  /usr/share/prewikka/cgi-bin/
  prewikka.cgi
</VirtualHost>
```

Hat alles geklappt, so sollte die URL *http://localhost/prewikka* nun den Startbildschirm des Webinterfaces zeigen. Als Default-Login steht der Admin-Account mit den Zugangsdaten "admin / admin" zur Verfügung. Natürlich sollte die oben dargestellte Apache-Konfiguration entsprechend angepasst werden, so dass der Server beispielsweise nur aus bestimmten Netzen erreichbar ist.

Den ersten Sensor einrichten

Was bringt das schönste Webinterface, wenn es keine Daten zum Anzeigen hat. Dies ändert sich jedoch in wenigen Minuten. Mit Prelude-LML kommt schließlich der erste Prelude-Sensor zum Einsatz. Dieser ist in der Lage, diverse Logdateien auszuwerten und auch selbst als zentraler Syslog-Server für andere Systeme und Geräte zu dienen. Diese sind dann nur noch so zu konfigurieren, dass neben dem lokalen Speichern der Logs diese auch an den zentralen Prelude-LML-Sensor gesendet werden. Dieser kann die Meldungen dann mit Hilfe diverser Rulesets auswerten und die Informationen gesammelt an den Prelude-Manager weiterleiten, der wiederum die Daten über Prewikka darstellt. Mit Hilfe von Prelude-LML lassen sich somit also Logs von Unix-Systemen, Routern, Switches, Firewalls und vielen anderen Geräten an zentraler Stelle bereitstellen. In diesem Artikel gehen wir davon aus, dass der Sensor auf dem gleichen Host wie der Prelude-Manager läuft. In produktiven Umgebungen macht es natürlich Sinn, mehrere Prelude-LML in diversen Netzwerk-Segmenten zu platzieren.

Neben der Konfiguration eines Sensors ist für diesen jeweils auch ein Schlüsselpaar zu erzeugen und der Sensor ist beim Manager anzumelden. Dies gelingt über den folgenden Aufruf:

```
# prelude-admin register prelude-lml
  "idmef:w admin:r" localhost -uid 0
  -gid 0

Generating 2048 bits RSA private
  key... This might take a very
  long time.
```

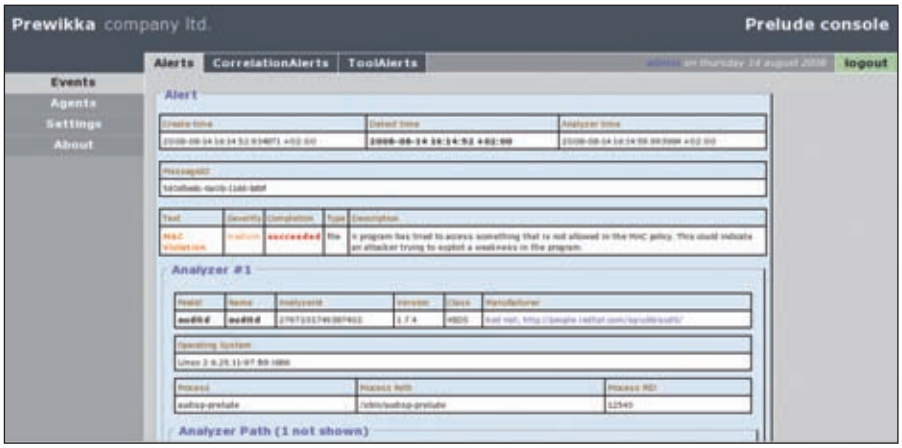


Bild 3: ...oder auch detaillierte Informationen zu einem bestimmten Event

```
[Increasing system activity will
  speed-up the process].
Generation in progress...
  X.+++++O....+++++O

You now need to start "prelude-
  admin" registration-server on
  localhost:
example: "prelude-admin registrati-
  on-server prelude-manager"

Enter the one-shot password provided
  on localhost:

Connecting to registration server
  (127.0.0.1:5553)... Authentication
  succeeded.
Successful registration to
  127.0.0.1:5553.
```

In einem anderen Fenster ist nun entsprechend ein Registration-Server zu starten. Dieser erzeugt eine Zufallszahl, die in dem ersten Fenster einzugeben ist:

```
# prelude-admin registration-server
  prelude-manager

The "aquto01a" password will be
  requested by "prelude-admin
  register"
in order to connect. Please remove
  the quotes before using it.

Generating 1024 bits Diffie-Hellman
  key for anonymous authenticati-
  on...
Waiting for peers install request on
  0.0.0.0:5553...
Waiting for peers install request on
  :::5553...

Connection from 127.0.0.1:45145...
Registration request for
  analyzerID="2990720184586729"
  permission="idmef:w
admin:r".

Approve registration? [y/n]: y

127.0.0.1:45145 successfully
  registered.
```

Damit ist die Registrierung des Sensors abgeschlossen. Weitere Sensoren sind auf die gleiche Art und Weise beim Prelude-Manager anzumelden. Nach einem *service prelude-lml start* sollte ein Blick auf das Prewikka-Webinterface bestätigen, dass der Sensor beim Prelude-Manager bekannt ist. Eine Konfiguration des Sensors kann nun über die Datei */etc/prelude-lml/prelude-lml.conf* erfolgen. Hier erfährt der Sensor beispielsweise, welche Logdateien er überwachen soll oder ob auf dem UDP-Port 514 auf eingehende Log-Meldungen zu achten ist.

Alternativer Sensor Snort

Um auch vor verdächtigen Aktivitäten im Netzwerk geschützt zu sein, bietet Prelude an, das bekannte Netzwerk-basierte IDS Snort [2] anzubinden. Snort ist eine Art Netzwerk-Sniffer, der den Netzwerk-Verkehr auf verdächtige Pakete hin überprüft. Diese Pakete identifiziert Snort anhand von Signaturen. Entsprechende Signatur-Dateien [3] lassen sich 30 Tage nach Erscheinen kostenlos von der Snort-Webseite herunterladen. Alternativ hilft das Tool Oinkmaster [4] mit einem automatischen Download mittels cron. Möchten Sie die Regeln schon unmittelbar nach deren Herausgabe nutzen, müssen Sie beim Hersteller Sourcefire ein kostenpflichtiges Abo dieser Regeln erwerben. Auch Snort kann mit einer MySQL-Datenbank im Backend arbeiten. Die Vorgehensweise ist identisch mit den Beispielen für den Prelude-Manager und Prewikka. Mit Hilfe der Datei */usr/share/doc/snort-2.8.5.1/create_mysql* aus dem RPM-Paket snort ist auch das notwendige Schema im Handumdrehen erstellt.

Über die Konfigurationsdatei */etc/snort/snort.conf* setzen Sie nun die wichtigsten Variablen entsprechend. Hierzu zählen beispielsweise "HOME_NET" und "EXTERNAL_NET". Auch das Interface, über das Snort auf den IP-Verkehr zgreift, und der Ordner mit den Signaturen sind korrekt anzugeben. In der Sektion vier der Datei bestimmen Sie schließlich, dass Snort sämtliche Meldungen an Prelude weiterleiten soll, dies geschieht über die Anweisung *output alert_prelude: profile=snort*. Ist die Datei soweit angepasst, startet das bekannte Spiel, der Sensor ist auf dem Prelude-Manager anzumelden. Hierzu ist wieder eine Registrierung möglich, die den Registrierungscode eines zusätzlich gestarteten Registrierungsservers benötigt.

Danach ist Snort als Prelude-Sensor einsatzbereit und überwacht das Netzwerk anhand der Konfigurationseinstellungen und der vorhandenen Angriffs-Signaturen. Neben einem Eintrag in der zuvor eingerichteten MySQL-Datenbank stellt Snort die generierten Logmeldungen nun auch über Prewikka bereit.

Protokolle mit dem Audit-Daemon erzeugen

Neben den bereits vorgestellten Sensoren kommen jetzt noch einige besonders interessante Konfigurationsmöglichkeiten zur Sprache. Da wäre zum einen die Integration des Linux Audit-Daemons [5] in das Prelude-Framework. Beim Audit-Daemon (auditd) handelt es sich um einen sehr leistungsfähigen Logging-Daemon mit umfangreichen Protokollmöglichkeiten. Hierzu zählen beispielsweise die folgenden Events beziehungsweise Subsysteme, die auf den Auditd zurückgreifen:

- Linux-Security-Modules (LSM) / SELinux
- Aufruf und Beendigung von System-Aufrufen
- Dateioperationen
- Prozess-Generierung

Zudem gibt es eine Reihe von Events, die der auditd automatisch protokolliert. Hierzu zählen beispielsweise Benutzer-An- und Abmeldungen. Eine detaillierte Liste aller Events zeigt der Aufruf von *ausearch -m*. Das Audit-System besteht aus mehreren Komponenten, wobei sich einzelne Teile davon durchaus deaktivieren lassen:

- Dem eigentlichen Framework im Kernel (kernel/audit.c und kernel/auditsc.c)
- Dem Audit-Daemon im User-Space für die Verarbeitung der Audit-Ereignisse
- Einem Event-Dispatcher, der Audit-Events in Echtzeit an andere Programme, beispielsweise an Prelude, weiterleitet.
- Weiteren Tools im User-Space zur Konfiguration und Verwaltung. Hierzu zählen audtictl, ausearch, aureport.

Der Audit-Daemon lässt sich grundsätzlich über zwei Dateien in */etc/audit/* konfigurieren: *auditd.conf* und *audit.rules*. Erstere legt allgemeine Informationen über den Dienst fest, die zweite enthält die eigentlichen Regeln darüber, was auf dem lokalen System alles zu protokollieren ist. Alternativ

ist es auch möglich, die Regeln mit Hilfe des Programms "auditctl" dynamisch zu setzen. Im Dokumentations-Ordner */usr/share/doc/audit-version/* finden sich bereits vorgefertigte Regeln, um dem Audit-Level bestimmter Schutzprofile (CAPP, LSPP, NISPOM) zu entsprechen. Diese können Sie bei Bedarf einfach nach */etc/audit/* kopieren und in *audit.rules* umbenennen. Mit dem Befehl *auditctl -s* sehen Sie die aktuellen Einstellungen des Audit-Systems:

```
# auditctl -s
AUDIT_STATUS: enabled=1 flag=1
  pid=2108 rate_limit=0 backlog_
  limit=1024
lost=0 backlog=0
```

Möchten Sie nun einfache Datei-Überwachungen einrichten, sogenannte File-Watches, geschieht dies mit dem Befehl

```
# auditctl -w /etc/audit/auditd.conf
  -p wa -k CFG_auditd.conf
```

Der Parameter "-w" gibt die zu überwachende Datei an, "-p" bestimmt den Zugriff auf die Datei (w=write, r=read, x=execute, a=Attribut-Änderung) und mit "-k" lässt sich ein Filter-Key mit dieser Regel verknüpfen. Mit Hilfe dieses Keys lassen sich audit-Meldungen später sehr leicht im Log finden und einer bestimmten Regel zuordnen.

Ändern Sie nun beispielsweise die Zugriffsrechte auf die Datei, so finden Sie hierfür einen entsprechenden Audit-Eintrag im Log:

```
type=SYSCALL msg=
  audit(1218578553.587:8099):
  arch=40000003 syscall=306
success=yes exit=0 a0=ffffff9c
  a1=90e48d8 a2=1b4 a3=90e48d8
  items=1
ppid=3431 pid=9603 auid=500 uid=0
  gid=0 euid=0 suid=0 fsuid=0 egid=0
  sgid=0
fsgid=0 tty=pts0 ses=1 comm="chmod"
  exe="/bin/chmod"
  key="CFG_auditd.conf"
```

Dank des bereits erwähnten Audit-Dispatchers ist es nun möglich, die gesammelten Log-Informationen zusätzlich an Prelude zu senden, anstatt diese nur in der Logdatei *audit.log* abzulegen. Notwendig ist hierzu das Paket "audispd-plugins". Nach dessen Installation müssen Sie das Plug-in aktivieren. Dies geschieht durch das Setzen der Anweisung "active=yes" in der Konfigurationsdatei */etc/audisp/plugins.d/au-prelude.conf*. Nach einem Neustart mittels *service auditd restart* sendet dieser nun also sämtliche Log-Meldungen auch an den Prelude-Manager. Eine zusätzliche Registrierung ist in diesem Fall nicht notwendig.

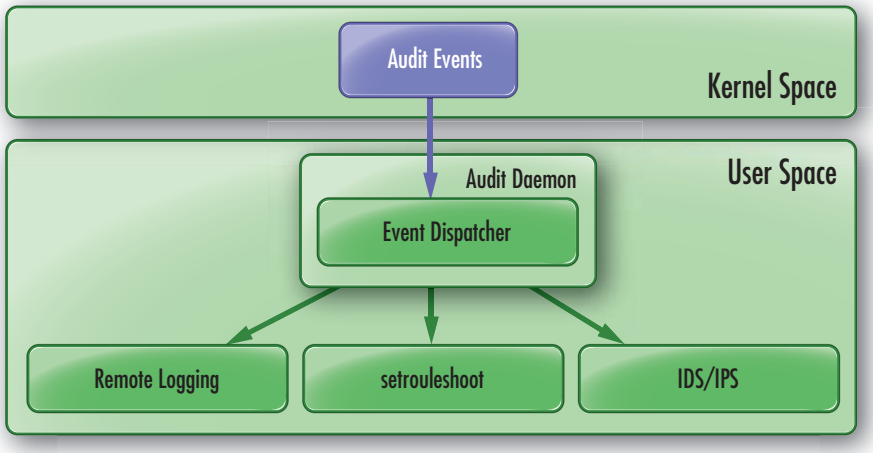


Bild 4: Der Audit-Dispatcher leitet Event-Meldungen in Echtzeit an andere Programme weiter

Hilfreiche Pop-ups für den Admin

Neben dem auditd gibt es einen weiteren sehr interessanten Sensor mit dem Namen Prelude-Notify. Hierbei handelt es sich um ein kleines Applet für den GNOME-Desktop, das eintreffende Nachrichten im Prelude-Manager unmittelbar mit einem Pop-up-Fenster sichtbar macht. Somit bekommt der Administrator direkt eine visuelle Nachricht und kann sofort Prewikka für detaillierte Informationen abfragen. Das Tool steht nach der Installation des Paketes "prelude-notify" zur Verfügung. Für diesen Sensor ist wieder eine Registrierung auf dem Prelude-Manager notwendig. Ist diese erfolgreich abgeschlossen, ist das Applet über das Gnome-Menü unterhalb von System-Tools aufzurufen und zu starten. Eine Ameise in der Task-Leiste des Desktops bestätigt, dass das Tool aktiv ist.

Natürlich bietet Prelude noch eine Vielzahl weiterer Sensoren - die hier vorgestellten sind nur eine kleine Auswahl. Einen Blick wert sind sicherlich auch Samhain als Host-basiertes IDS und OSSEC [6] für die Überwachung von Windows-Systemen. Dank der umfangreichen API ist es problemlos möglich, Prelude auch in eigene Tools zu integrieren. Die sehr umfangreiche Dokumentation auf der Prelude-Webseite leistet hier wertvolle Dienste [7].

Fazit

Mit Prelude steht ein sehr leistungsstarkes und extrem flexibles Intrusion-Detection-System zur Verfügung. Es ist bei vielen Unternehmen weltweit im Einsatz, sicherlich nicht nur wegen der umfangreichen Features, die das Tool bietet, sondern auch weil der Hersteller guten Support leistet und eine vorbildliche Dokumentation für sämtliche Komponenten zur Verfügung stellt [8]. Wer außerdem eine programmierbares Tool sucht, um es entsprechend in die eigene Landschaft zu integrieren, der ist mit Prelude auf der sicheren Seite. *(dr)*

Link-Codes

[1] Prelude-Webseite
BOP11

[2] Snort-Webseite
BOP12

[3] Snort-Regeln zum Herunterladen
BOP13

[4] Oinkmaster auf Sourceforge
BOP14

[5] Auditd-Projektseite
BOP15

[6] OSSEC How-To
BOP16

[7] Prelude-Dokumentation
BOP17

[8] Prelude Entwickler-Dokumentation
BOP18

Neuerungen in SQL Server "Denali"

Datenbank in der Cloud

von Thomas Joos

Aktuell arbeitet Microsoft mit Hochdruck am Nachfolger von SQL Server 2008 R2, der den Codenamen Denali trägt. Zahlreiche Neuerungen sollen dem Administrator das Leben noch einfacher machen - dazu gehören eine ausgebaute Hochverfügbarkeit und Verbesserungen bei der Datenbankmigration. Im nächsten Jahr soll der SQL Server 2012 dann erscheinen. Warum sich ein Upgrade lohnt und welche Vorteile Denali mitbringt, lesen Sie in diesem Beitrag.

Die ausgebaute Hochverfügbarkeit dürfte sicherlich eines der Killerfeatures von SQL Server Denali sein. So gibt es in der neuen Version die Funktion "AlwaysOn". Diese fasst die bisherigen Hochverfügbarkeitslösungen "Cluster", "Datenbankspiegelung" und "Log-Shipping" zusammen und erweitert diese. Administratoren müssen damit nicht mehr verschiedene Hochverfügbarkeitslösungen verwalten. AlwaysOn basiert auf Verfügbarkeitsgruppen, die Sie im SQL Server Management Studio anlegen. Diese enthalten mehrere SQL Server-Datenbanken und stellen diese hochverfügbar zur Verfügung. Im Gegensatz zu den Vorgängerversionen können Sie unter Denali also mehrere Datenbanken auf einmal hochverfügbar über Gruppen konfigurieren, was die Konfiguration beschleunigt und vereinfacht. Dazu nutzt die Technik entweder einen gemeinsamen Datenträger, also Clusterfunktionen, getrennte Datenträger mit Datenbankspiegelung oder die Replikation - sowohl asynchron als auch synchron.

Wer sich die neue Version genauer ansehen will, für den bietet Microsoft die Betaversion CTP3 an [1]. Für den Download sollten Sie Internet Explorer verwenden, da dieser den Download-Manager unterstützt, den die Download-Seite des CTP3 als ActiveX-Element im Browser installiert. Wie Sie Denali installieren, lesen Sie im TechnNet [2].

Hochverfügbarkeit mit AlwaysOn

Die Steuerung hierzu findet im SQL Server Management Studio über die Verfügbarkeitsgruppen statt. Von Datenbanken erstellen Sie somit auf einfachem Weg mehrere Replikate. Um eine Hochverfügbarkeit herzustellen, können Sie mit der aktuellen Betaversion CTP3 bis zu eine primäre und vier sekundäre Repliken erstellen. Primäre Replikate liegen zum Beispiel in einem leistungsfähigen lokalen Datenspeicher, sekundäre sind im Netzwerk gesichert. Failover führen Sie zwischen den Replikaten manuell, automatisch oder auch geplant durch.

Replikate können Sie auch als lesbare Kopie zur Verfügung stellen, im Gegensatz zu gespiegelten Datenbanken. Die Einstellung dazu nehmen Sie beim Anlegen der Verfügbarkeitsgruppe vor. Sie können für jede Datenbank der Verfügbarkeitsgruppe diese Einstellung getrennt festlegen. Die Kopien lassen sich dann zum Beispiel in Reporting Services einbinden, was die produktive Datenbank entlastet, weil Anwender Berichte aus der Kopie erstellen und die produktive Datenbank nicht belasten.

Basis der Verfügbarkeitsgruppen ist die Failovercluster-Rolle in Windows Server. Allerdings benötigen Sie nicht zwingend einen gemeinsamen Datenträger für den Cluster, sondern können auch mit getrennten Datenträgern arbeiten. Sie fassen über diesen Weg die beteiligten SQL-Server in einem Cluster zusammen, deren Datenbanken Sie hochverfügbar zur Verfügung stellen möchten. Auf den jeweiligen Servern installieren Sie SQL Server Denali mit einer eigenen Instanz. Einzelne Datenbanken auf den Datenbankservern fassen Sie dann zu Verfügbarkeitsgruppen zusammen. Dazu müssen Sie auf den Servern noch den Failover-Clusterdienst installieren, benötigen also für die Funktion die Enterprise Edition von Windows Server 2008 R2 oder Windows 8 Server.

Exchange Server 2010 nutzt diese Technik bereits auf ähnlichem Weg bei den Database Availability Groups (DAG). Auch die Replikation zwischen verschiedenen Rechenzentren ist möglich, natürlich auch verschlüsselt. All diese Techniken sind Bestandteil von AlwaysOn. Clients können über diesen Weg auch mit einem einzelnen Namen oder einer einzelnen IP-Adresse auf SQL zugreifen, genauso wie bei einem normalen Cluster.

Eine weitere neue Funktion im Bereich der Hochverfügbarkeit in SQL Server Denali sind "Contained Databases". Diese vereinfachen das Verschieben kompletter Datenbanken mit allen abhängigen Objekten zwischen verschiedenen Servern. Die Datenbanken enthalten zusätzlich die Benutzeranmeldungen und andere temporäre Objekte, die für den Betrieb notwendig sind. Dadurch lassen sich Datenbanken sehr schnell zwischen Servern verschieben, weil alle Daten direkt in der entsprechenden Datenbank gespeichert sind und Sie beim Verschieben nicht auch noch auf die Benutzerkonten achten müssen, die für die Datenbank angelegt sind. Große Datenbanken lassen sich in SQL Server Denali mit bis zu 15.000 Partitionen aufbauen, was ebenfalls der Stabilität und der Leistung dient.

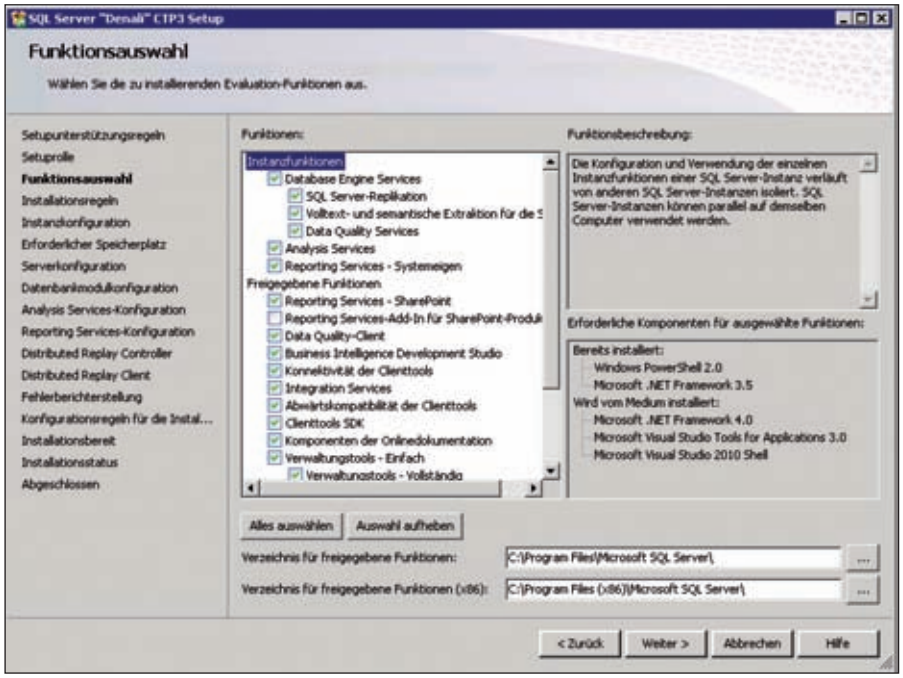


Bild 1: Das Setup von Denali CTP3 erlaubt eine detaillierte Auswahl der Funktionen

Beschleunigte Business Intelligence

Microsoft verspricht vor allem einen extremen Leistungszuwachs des neuen Datenbankservers. Auch im Bereich Business Intelligence bietet der neue SQL-Server zahlreiche Neuerungen, etwa die neue interaktive, webbasierte Datenanalyse mit dem Codenamen "Crescent" oder die neuen "Data Quality Services". Bei Letzteren handelt es sich um eine neue Komponente von SQL Server, die Verfahren wie Data Clensing und Data Matching verbessern soll. Crescent dagegen ist ein neues, interaktives und webbasiertes Werkzeug zur Datenanalyse. Das Tool ermöglicht zum Beispiel die webbasierte Analyse und das Erstellen von Berichten via Silverlight. Die Erstellung ist sehr simpel, die Berichte sehen ansprechend aus. In der Version CTP3 können Sie Crescent aber nur für Analysis Services-Modelle nutzen, die tabellarisch konfiguriert sind.

Sie benötigen für die Nutzung von Crescent die Funktion PowerPivot für SharePoint und damit einen SharePoint Server 2010 SP1, um die Funktion zu testen. Wie Sie bei der Installation von SharePoint Server 2010 SP1 dazu vorgehen müssen, lesen Sie im MSDN [3]. Nach der Integration können berechtigte Anwender selbst über eine eigene Webseite und Silverlight Berichte erstellen.

Mit einem neuen spaltenbasierten Indextyp (Columnstore Indizes) will Microsoft Abfragen in Data Warehouses beschleunigen. Vor allem bei Aggregationen lassen sich dadurch Leistungssteigerungen erzielen, da Sie sich das Durchsuchen der kompletten Baumstruktur der Daten ersparen können. Im neuen Indextyp speichern Sie die Daten sehr hoch komprimiert, jede Spalte des Index einzeln. Im Vergleich zur zeilenweisen Speicherung des Index steigt die Leistung hierbei. Dadurch ist die von der Festplatte zu lesende Datenmenge sehr gering, was natürlich merklich mehr Performance bringt. Der durchsuchbare Index ist darüber hinaus direkt im Arbeitsspeicher hinterlegt. Dies ist möglich, da Crescent auf die Vertipaq-Technik von PowerPivot zurückgreift.

SQL Server geht online

SQL Server Denali soll auch eine bessere Anbindung an das Internet bieten und als Cloud-Dienst arbeiten. Hier können Unternehmen entweder mit dem neuen Hyper-V 3.0 in Windows 8 Server eine Private Cloud aufbauen oder Daten zwischen einem lokal betriebenen SQL-Server und SQL Azure austauschen. Microsoft arbeitet dazu parallel an der neuen Entwicklungsumgebung mit dem Projektnamen "Juneau". Diese soll identische Entwicklungsmöglichkeiten für SQL

Galileo Computing

Portofrei im Web bestellen [D], [A]

Microsoft SharePoint Server 2010

- Planen, Einrichten und Betreiben von SharePoint
- Business Intelligence, Collaboration, Portale, Informationskonsolidierung
- Entwickeln für SharePoint

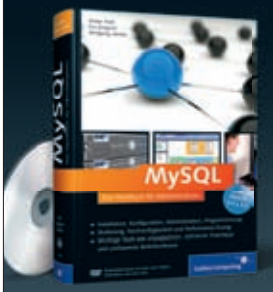
1.100 S., 2. Auflage 2011, 59,90 €
» www.galileocomputing.de/2445

Business Intelligence mit SharePoint 2010

- Administration, Konfiguration, Integration
- Unternehmensprozesse mit SharePoint und SQL-Server optimal abbilden
- SAP-Anbindung, SharePoint Insights, PowerPivot, Access u.v.m.

625 S., 2011, 59,90 €
» www.galileocomputing.de/2449

MySQL



- Installation, Konfiguration, Administration
- Skalierung, Hochverfügbarkeit und Performance-Tuning
- Wichtige Tools wie »mysqladmin«, zahlreiche Praxistipps und umfassende Befehlsreferenz

750 S., 2011, mit DVD, 49,90 €
» www.galileocomputing.de/2533

Citrix XenApp 6 und XenDesktop 5

- Planung, Installation, Konfiguration und Verwaltung
- Alle Editionen von XenApp 6 und XenDesktop 5
- Inkl. Best Practices und Troubleshooting

608 S., 4. Auflage 2011, 59,90 €
» www.galileocomputing.de/2465

www.GalileoComputing.de

booksonline

» www.facebook.com/GalileoPressVerlag
» www.twitter.com/Galileo_Press

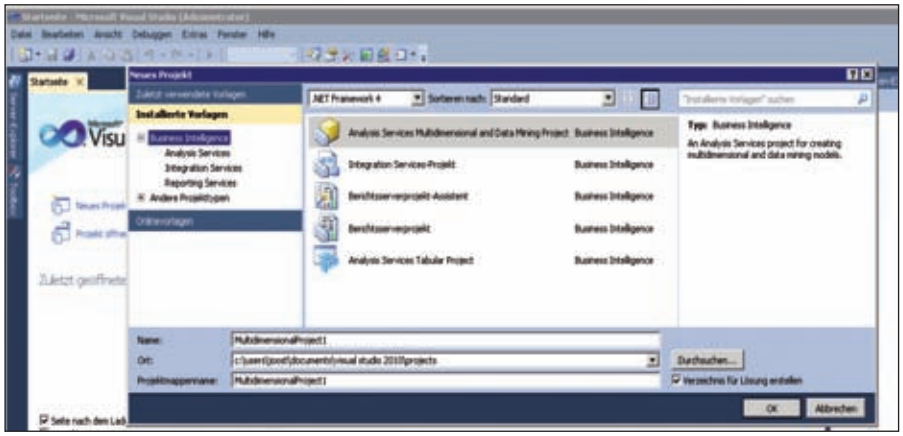


Bild 2: Das Entwickeln von Datawarehouses ist mit dem neuen SQL Server Business Intelligence Studio möglich

Server Denali, SQL Azure und für Business Intelligence bieten und auf Visual Studio 2010 aufbauen.

Mit dem neuen SQL Server Business Intelligence Studio entwickeln Sie wesentlich leichter und schneller Datawarehouses. Das Tool baut auf Visual Studio 2010 auf und gehört ebenfalls zum Projekt Juneau. Auch zum Projekt gehören weitere Entwicklungstools für SQL-Server, die zusammen mit SQL Server Denali erscheinen sollen. Grundlage aller Tools soll Visual Studio 2010 werden, so dass Entwickler nur noch eine einzelne Oberfläche benötigen, keine verschiedenen Tools mit unterschiedlichen Programmiersprachen und Oberflächen. Die Zusammenarbeit mit PHP und Java ist in SQL Server Denali zudem deutlich verbessert.

Dateizugriff in BLOBs von jeder Anwendung aus

Große Datenmengen lassen sich in SQL Server Denali besser in das Dateisystem auslagern, aber weiterhin mit SQL-Abfragen erfassen. Seit SQL Server 2008 gibt es die Möglichkeit, große Dateien nicht in der Datenbank zu speichern, sondern direkt im Dateisystem. Diese Technik wird "Filestream" genannt. Die ausgelagerten Dateien, zum Beispiel Videos oder sehr große Dokumente, sind weiterhin mit SQL-Mitteln erreichbar, gleichzeitig bleiben die Datenbankdateien übersichtlich. Der Nachteil dieser Technik ist jedoch, dass die Daten nur über SQL zugänglich sind, auch wenn sie im Dateisystem gespeichert sind. Das ändert sich in SQL Server Denali.

Filetables, eine weitere neue Funktion in Denali, ermöglichen über Dateifreigaben oder Programme, direkt auf Daten, die in Filesstreams gespeichert sind, zuzugreifen. Das heißt, Anwender oder Programme können direkt auf die Datei zugreifen, zum Beispiel über Office-Programme oder den Windows Explorer. Trotzdem bleiben die Daten im SQL-Zugriff und sind durch die SQL-Sicherung und -Volltextsuche erfasst. Administratoren müssen diesen Zugriff aber erst erlauben, standardmäßig ist die Funktion nicht aktiviert. Um den Zugriff zu gestatten, muss ein nicht-transaktionaler Zugriff erlaubt werden. Das geht schreibend oder nur lesend.

Externe Schreibzugriffe lassen sich allerdings nicht durch Rollback-Vorgänge rückgängig machen, da sie vollkommen nicht-transaktional sind. Greifen Sie jedoch transaktional auf einen nicht-transaktional-aktivierten Filestream zu, stehen auch Rollback-Funktionen zur Verfügung. Filetables erlauben keine Erweiterung ihres Schemas oder das Anpassen von Spalten. Trigger lassen sich dagegen hinzufügen. Das Schema der Filetables enthält die Eigenschaften, die Dateien in Windows erhalten können, wie schreibgeschützt, versteckt oder komprimiert.

Schnellere Suche, bessere Ergebnisse

Die semantische Suche bietet Volltextabfragen nach Ähnlichkeiten, zum Beispiel Begriffe wie "zeige mir ähnliche Dokumente wie das geöffnete". Außerdem können Sie in der Volltextsuche auch nach Metadaten von Dokumenten oder deren Eigenschaften, wie zum Beispiel Titel oder Autor suchen lassen. Dazu legen Sie eine Liste für die Datenbank an, nach welchen Eigenschaften Sie suchen wollen. Erstellen Sie einen neuen Index, berücksichtigt Denali die Eigenschaften in der Liste und ermöglicht auch Suchen nach diesen Eigenschaften. Verwenden Sie in TransactSQL die NEAR-Option, können Sie eingeben, in welchem Abstand die Worte auftauchen sollen, die Sie mit NEAR erfassen, zum Beispiel "Artikel" und "Schrauben". Sie können auch mehr als zwei Worte verwenden und den Abstand zwischen dem ersten und letzten Wort angeben.

Die Nutzung geografischer Daten, die bereits in SQL Server 2008 R2 verfügbar sind, soll jetzt die gesamte Erde umfassen, was angesichts der Globalisierung durchaus hilfreich sein kann, um etwa den Vertrieb zu steuern oder zu analysieren. SQL Server 2008 R2 kann hier nur Daten einer Halbkugel zusammenfassen, Denali den gesamten Globus. Denali soll sich auch in der Core-Version von Windows 8 Server oder Windows Server 2008 R2 installieren lassen. Somit steht der Datenbank mehr Leistung zur Verfügung, da Core-Server weit weniger Performance verbrauchen als vollwertige Installationen. SQL Server 2008 R2 unterstützt diese Möglichkeit noch nicht.

Verbesserungen in TransactSQL und Verwaltung

In TransactSQL können Sie mit Denali Sequences erstellen, also Zähler für bestimmte Abfragen zur Durchnummerierung. Diese bieten zum Beispiel die Möglichkeit, Zahlenfolgen auch außerhalb von Tabellen zur Verfügung zu stellen. Diese Zähler für TransactSQL funktionieren dabei über Tabellengrenzen hinweg. Ein Vorteil von Sequences ist damit die Möglichkeit, eindeutige IDs zu erstellen. Offsets ermöglichen ferner, Teile eines Suchergebnisses abzufragen, um bessere Ausgaberesultate zu erzielen. Mit der Technik können Sie gezielt einzelne Zeilen aus Tabellen auslesen und darstellen lassen.

Denali bietet neue Benutzerrollen, die auch benutzerdefiniert sein können, eine verbesserte Überwachung und ein Stan-

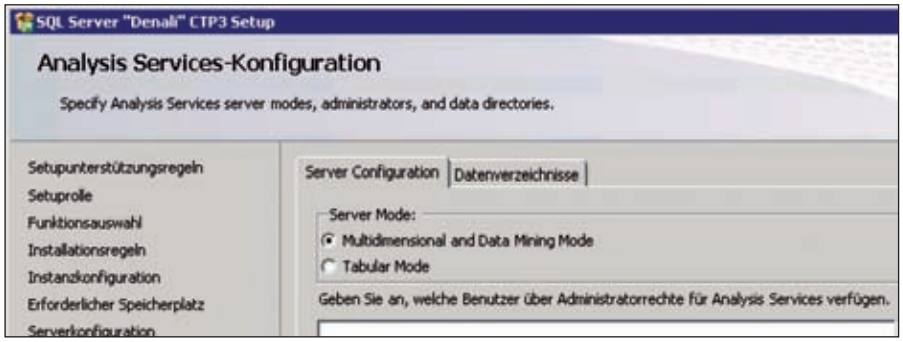


Bild 3: Beim Setup legen Sie den Betriebsmodus der Analysis Services fest

dardschema für Windows-Gruppen. Künftig soll sich der Server auch in der PowerShell 2.0 verwalten lassen, und zwar nicht nur die Datenbanken selbst, sondern auch die Analysis Services und PowerPivot für SharePoint. Auch die Wiederherstellung dürfte schneller und sicherer ablaufen. Mit dem neuen Database Recovery Advisor sollen auch weniger geübte Administratoren schneller Wiederherstellungsvorgänge durchführen können.

Verbesserte Analysis-, Reporting- und Integration Services

Eine weitere Neuerung ist ein spaltenbasierter Speichermodus, der auf der VertiPaq Engine aufbaut. Diese wurde bereits mit PowerPivot eingeführt. Eine Analysis Services-Instanz verwendet im neuen SQL-Server das tabellarische oder das multidimensionale Modell. Diese Einstellung legen Sie bei der Installation der Instanz fest. Mit dieser Technik lasen sich Projekte besser und schneller erstellen.

Für PowerPivot hält Denali einige neue Datenanalyse-Funktionen (DAX) und eine bessere Integration in SharePoint bereit. Der SharePoint Mode von Reporting Services sowie Crescent lassen sich als SharePoint Shared Service integrieren. Claims Authentication ist damit ein unterstütztes Szenario. Mit den neuen Data Alerts können sich Anwender automatisch über Änderungen in Berichten informieren lassen. Berichte lassen sich in SQL Server Denali im Office 2007/2010-Format erstellen. Auf diese Weise können Sie größere und umfassendere Berichte anfertigen. Die Nutzung der Office 2003-Formate ist aber auch noch möglich.

Integration Services können in Projekten mehrere Pakete zusammenfassen, die eine zusammengehörige Konfiguration ermöglichen. Das heißt, einzelne Pakete sind nicht mehr notwendig, sondern lassen sich kombinieren. Mit dem neuen Integration Services-Dienst können Sie zentral alle Projekte und Pakete ausführen oder verwalten. Mit der neuen Object Impact and Data Lineage Analysis verfolgen Sie Änderungen in einzelnen Datenquellen. Beim Erstellen von neuen Paketen stehen neue Assistenten zur Verfügung, die vor allem die Anbindung von Datenquellen erleichtern.

Fazit

SQL Server Denali bietet viele Neuerungen, die durchaus eine Migration rechtfertigen. Besonders Unternehmen, die Business Intelligence nutzen, erhalten bessere Werkzeuge, zuverlässigere Daten und eine Leistungssteigerung. Die Möglichkeiten zur Hochverfügbarkeit hat Microsoft deutlich verbessert und die Administration erleichtert. Administratoren sollten einen Blick auf die Testversion werfen, die bereits zahlreiche der beschriebenen Funktionen unterstützt. Es ist zu erwarten, dass SQL Server Denali vor allem als virtueller Server mit Windows 8 Server eine deutliche Leistungssteigerung erreichen kann. *(dr)*

Link-Codes

[1] Betaversion CTP3
BAP51

[2] TechNet-Anleitung zur Denali-Installation
BAP52

[3] SharePoint Server 2010 SP1
BAP53

Link-Codes eingeben auf www.it-administrator.de

iladministrator
Das Magazin für professionelle System- und Netzwerkadministration

Worüber Administratoren morgen reden

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

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

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

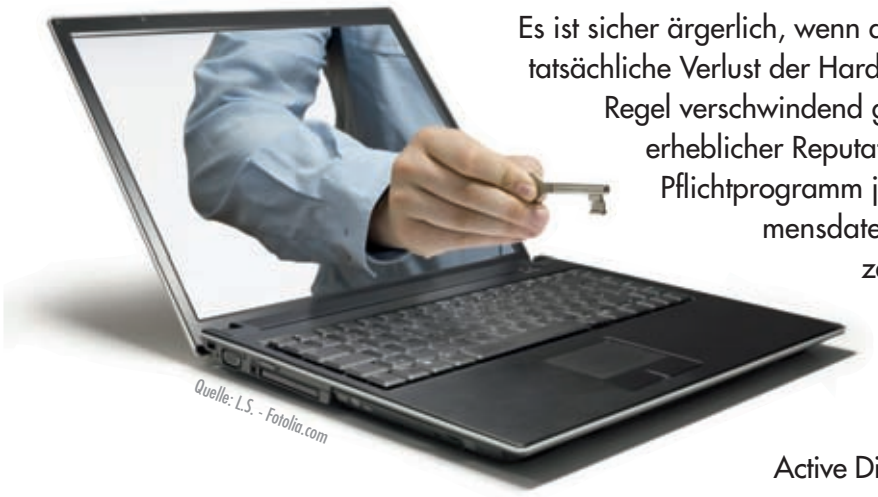
Jetzt einfach und kostenlos bestellen unter:

www.it-administrator.de/newsletter

Windows-Laufwerke mit BitLocker und TPM-Chip verschlüsseln

Eingebaute Sicherheit

von Thomas Gronenwald



Es ist sicher ärgerlich, wenn das eigene Notebook verschwindet. Doch der tatsächliche Verlust der Hardware gegenüber den Folgeschäden ist in der Regel verschwindend gering. Neben dem Daten- droht oft auch ein erheblicher Reputationsverlust. Nicht nur deshalb gehört es zum Pflichtprogramm jeder IT, den Zugriff auf vertrauliche Unternehmensdaten und die dazugehörige Hardware zu schützen und entsprechend zu verschlüsseln. Mit BitLocker bietet Microsoft hierfür ein durchaus praktikables und sicheres Verfahren an – insbesondere in Kombination mit TPM-Chips. Verwalten lässt sich das Ganze via Active Directory. Wie das geht, zeigt dieser Workshop.

Daten auf einem verlorenen oder gestohlenen Computer sind durch das Ausführen von frei verfügbaren Tools oder durch das Einbauen der Festplatte in einen zweiten Computer kriminellen Personen schutzlos ausgesetzt. Durch eine Verschlüsselungslösung, kombiniert mit einer Pre-Boot-Authentifizierung, die sowohl die Betriebssystem- als auch die Datenpartitionen entsprechend schützt, ist es möglich, einen Missbrauch zu minimieren.

Zusammenarbeit von TPM und BitLocker

Mit der seit Windows Vista eingeführten und bereits standardmäßig in der Ultimate und Enterprise-Version integrierten Windows BitLocker-Verschlüsselung wird der nicht autorisierte Zugriff auf verloren gegangene oder gestohlene Computer durch die Kombination von zwei wichtigen Verfahren erschwert:

1. Verschlüsselung von Betriebssystem- und Datenpartition: BitLocker Drive Encryption (BDE) verschlüsselt alle auf der Betriebssystempartition vorhandenen Benutzer- und Systemdateien, einschließlich der Auslagerungsdateien. Zudem ermöglicht BitLocker die Verschlüsselung von Datenpartitionen.
2. Trusted Platform Module (TPM), Version 1.2: Auf Systemen mit einem TPM in der Version 1.2 verwendet BitLocker dessen Sicherheitsfunktionen, um sicherzustellen, dass der Zugriff auf Daten nur dann möglich ist, wenn die Startkomponenten des Computers unverändert sind und sich der verschlüsselte Datenträger noch im Originalcomputer befindet.

Der Einsatz von BDE ist nicht unter allen Windows-Versionen möglich, sondern lediglich unter:

- Windows Vista Enterprise
- Windows Vista Ultimate
- Windows 7 Enterprise
- Windows 7 Ultimate
- Windows Server 2008
- Windows Server 2008 R2

Das Prinzip des unterstützten TPM ist einfach: Während des Bootvorgangs erfasst das TPM alle grundlegenden Gesichtspunkte der Hardwarekonfiguration. Als Ergebnis liefert es eine kryptografische Prüfsumme, einen sogenannten Hash. Veränderungen, wie sie beispielsweise bei Systemänderungen in der Hardware auftreten – etwa durch den Ausbau der Festplatte oder ein Firmware-Update des BIOS –, schlagen sich dadurch in veränderten Hash-Werten nieder. Das System kann daher nicht von unautorisierten Personen gestartet werden. Um die Betriebssystempartition verschlüsseln zu können, werden zwei Partitionen mit dem NTFS-Dateisystem benötigt. Eine Systempartition mit 100 MByte Speicherkapazität wird zum Starten des Computers verwendet und verbleibt unverschlüsselt. Besitzt der Computer keine zwei Partitionen, legt BitLocker diese während des Setups an.

BitLocker im Detail

Microsoft empfiehlt zusätzlich zur Verschlüsselung die Eingabe einer PIN. Zusätzlich oder alternativ dazu kann das Starten des Systems auch davon abhängig gemacht werden, ob ein USB-Datenträger mit einer entsprechenden Schlüsseldatei eingesteckt ist. Bei Computern ohne TPM ist keine Eingabe einer PIN möglich. Hier lässt sich lediglich eine Schlüsseldatei auf einem USB-Datenträger ablegen und das Starten des Systems von diesem abhängig machen. Zur Verschlüsselung verwendet BDE den Advanced Encryption Standard (AES), eine symmetrische Blockchiffre mit einer Blocklänge von 128 Bit. Die eingesetzte Schlüssellänge ist dabei variabel und kann eine Länge von 128, 192 oder 256 Bit betragen.

BDE speichert die Recovery-Informationen zur Entschlüsselung der Partition

während des Verschlüsselungsprozesses auf einen vorher zu wählenden nicht verschlüsselten oder lokalen Datenträger. Ebenso ist es möglich, die Wiederherstellungsschlüssel auszudrucken und an einem sicheren Ort aufzubewahren. Zusätzlich empfiehlt es sich, die sogenannten Wiederherstellungsschlüssel innerhalb der Active Directory Domain Services (AD DS) zu speichern. Hierzu legt BitLocker innerhalb des Computerobjektes für jede verschlüsselte Partition einen eigenen Wiederherstellungsschlüssel ab. Wird auch ein TPM-Chip genutzt, so wird dessen Recovery-Passwort ebenfalls im AD abgelegt. Für ein Recovery ist also entweder das originale, selbst festgelegte Passwort oder aber das hinterlegte Recovery-Passwort notwendig.

Wiederherstellung dank Notfall-Key

Im Unternehmensnetzwerk muss jederzeit sichergestellt werden, dass eine verschlüsselte Partition unter allen Umständen wieder entschlüsselt werden kann. Sei es bei Vergessen der PIN zur TPM-Authentifizierung, bei Vergessen des Passworts zur Verschlüsselung oder bei einem Hardwaredefekt – ein Recovery beziehungsweise eine Entschlüsselung der Daten muss stets gewährleistet werden können.

Hierzu wird bei jeder Verschlüsselung ein Wiederherstellungsschlüssel erstellt. Der Wiederherstellungsschlüssel kann dabei sowohl auf einem USB-Stick als auch an einem durch den Administrator festgelegten Speicherort abgelegt werden. Alternativ kann dieser auch ausgedruckt und an einem sicheren Ort aufbewahrt werden. In jedem Szenario ist dafür Sorge zu tragen, dass dieser Schlüssel unabhängig vom System an einem sicheren Ort aufbewahrt wird. Innerhalb einer Active Directory Domäne empfiehlt es sich daher, den Wiederherstellungsschlüssel sowie alle TPM-Besitzerkennwörter im Active-Directory zu hinterlegen.

Vorabtest zur Sicherheit

Wie auch bei anderen Technologien, empfiehlt es sich zwingend, alle Einstellungen vorab in einer Testumgebung zu testen und diese im Anschluss daran in die eigentliche Produktivumgebung zu überführen. In unserem Szenario greifen wir auf eine homogene Windows Server 2008 R2-Domänenstruktur mit zwei Domain Controllern (Windows Server 2008 R2 Standard, Service Pack 1) zurück. Ebenfalls nutzen wir das vorab bereits installierte Feature "BitLocker-Wiederherstellungskennwort-Viewer für Active Directory". Dieses installieren Sie im Server-Manager unter "Features". Sie benötigen es im weiteren Verlauf zum Auslesen unserer Wiederherstellungskennwörter. Hierdurch werden die Eigenschaften der Computerobjekte durch den Eintrag "BitLocker Wiederherstellung" erweitert. Ebenso erhalten Sie hierdurch einen zusätzlichen Menüeintrag zum Suchen von Wiederherstellungsinformationen innerhalb der AD DS. In einer Windows Server 2003-Domäne sind noch weitere vorbereitende Schritte wie die Erweiterung des Active Directory-Schemas notwendig. Diese benötigen wir innerhalb einer Windows Server 2008 R2-Domäne jedoch nicht. Weitere Informationen hierzu finden Sie unter anderem im Microsoft BitLocker-Betriebshandbuch unter [1].

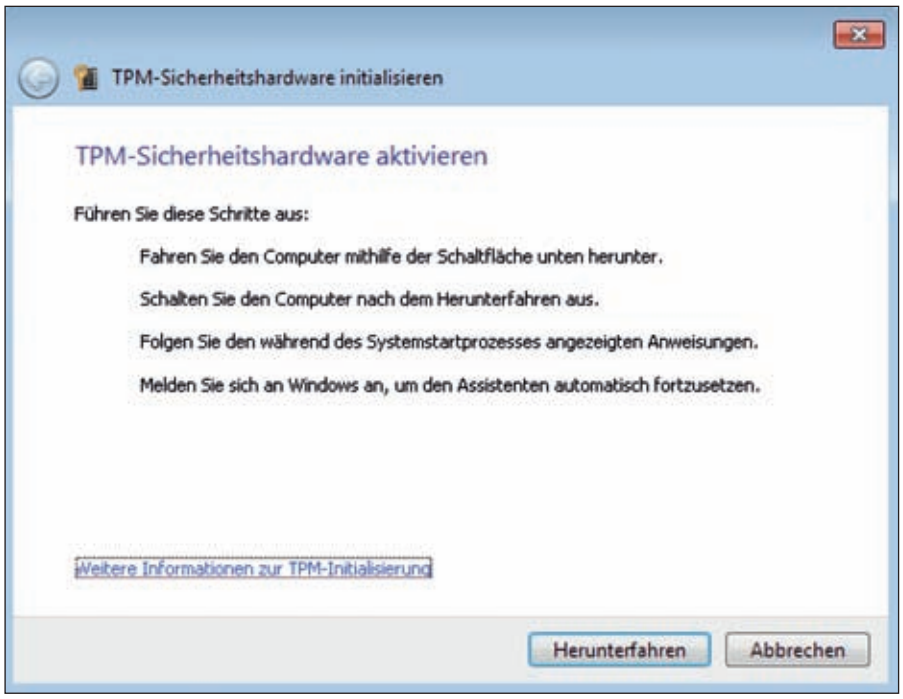


Bild 1: Um den TPM-Chip zu nutzen, müssen Sie diesen erst aktivieren

Schritt 1: Group Policy Object für TPM erstellen

Im ersten Schritt ist es nun notwendig, ein geeignetes Group Policy Object (GPO) zu erstellen und mit der richtigen Organisationseinheit (OU) unserer Computerobjekte zu verknüpfen. Hierzu öffnen Sie die Gruppenrichtlinienverwaltung und navigieren zu den TPM-Diensten unter "Computerkonfiguration / Administrative Vorlagen / System / Trusted Platform Module-Dienste". Wählen Sie die Richtlinie "TPM-Sicherung in Active Directory-Domänendienste aktivieren". Ebenso aktivieren Sie die Option "TPM-Sicherung in AD DS erforderlich".

Diese Richtlinieneinstellung ermöglicht das Speichern von TPM-Besitzerinformationen im AD DS. Hierbei umfassen die TPM-Besitzerinformationen einen kryptografischen Hash des TPM-Besitzerkennworts. Aktivieren Sie diese Richtlinieneinstellung, werden die TPM-Besitzerinformationen automatisch und im Hintergrund in AD DS gesichert. Hierdurch lässt sich ein TPM-Besitzerkennwort nur dann festlegen oder ändern, wenn der Computer Mitglied der Domäne ist und auch die entsprechende Konnektivität besitzt. Nur dann lassen sich Sicherung und TPM-Aktivierung erfolgreich ausführen.

Schritt 2: TPM konfigurieren

Damit Ihre Clients nun eigenständig ihre TPM-Benutzerschlüssel während der Aktivierung in ihr Computerobjekt schreiben können, ist es notwendig, ihnen die-

ses Recht zu delegieren. Hierzu öffnen Sie die Active Directory-Benutzer und -Computer-Verwaltungskonsole und weisen unserer OU die entsprechenden Berechtigungen zu. Delegieren Sie die Berechtigungen auf den Benutzer "Selbst" und wählen Sie im nächsten Fenster "Benutzerdefinierte Aufgaben zum Zuweisen erstellen" und anschließend "Computer"-Objekte und das Attribut "msTPM-OwnerInformation schreiben". Unter einem englischen Betriebssystem ist darauf zu achten, anstelle des deutschen Benutzers "Selbst" das englische Äquivalent "Self" zu nutzen. Hierzu bietet Microsoft auch ein entsprechendes Skript (*Add-TPMSelfWriteACE.vbs*) an, das diesen Schritt übernimmt. Nachteil hierbei ist jedoch, dass die Berechtigungen hiermit nur für die gesamte Domäne und nicht nur für eine definierte OU vorgenommen werden können. Auch hier ist darauf zu achten, den Benutzer gegebenenfalls zu ersetzten und den richtigen LDAP-Pfad zu nutzen. Vergeben Sie diese Berechtigungen nicht, erhalten Sie bei der TPM-Initialisierung auf dem Client in der Regel den Fehlercode "x0x80070005 - Zugriff verweigert".

Ein TPM befindet sich in der Regel in einem der folgenden vier Zustände:
- Ohne Besitzer und ausgeschaltet
- Ohne Besitzer und eingeschaltet
- Mit Besitzer, aber ausgeschaltet
- Mit Besitzer und eingeschaltet

Bevor das TPM für die Sicherheit des Computers sorgen kann, muss es im BIOS eingeschaltet werden (standardmäßig ist TPM deaktiviert) und einen Besitzer haben. Der Vorgang, bei dem sichergestellt wird, dass das TPM eingeschaltet ist und einen Besitzer aufweist, wird Initialisierung genannt. Während dieser erstellt das TPM neue Stammschlüssel, die es selbst verwendet. Nach der Aktivierung im BIOS starten wir unseren Client neu und prüfen, ob der Treiber innerhalb des Geräte-Managers ordnungsgemäß installiert und das TPM einsatzbereit ist. Anschließend öffnen Sie die TPM-Verwaltung mit *tpm.msc* und initialisieren unsere TPM-Hardware. Folgen Sie nun den Anweisungen des Assistenten und fahren Sie den Client anschließend herunter. Während des nächsten Boot-Vorgangs wird eine Bestätigungseingabeaufforderung angezeigt, um zu überprüfen, ob ein Benutzer physikalischen Zugriff auf den Computer hat. Auf diese Weise stellt das System sicher, dass keine Schadsoftware versucht, das TPM zu aktivieren.

Nach der Bestätigung und dem Neustart aktivieren Sie in der TPM-Verwaltung Ihre TPM-Hardware und speichern das TPM-Benutzerkennwort an einem sicheren Ort ab. In diesem Schritt werden durch die vorab erstellte Gruppenrichtlinie die TPM-Informationen im Active Directory Computer-Attribut "msTPM-OwnerInformation" hinterlegt. Um dies zu validieren, öffnen Sie auf einem Ihrer Domain Controller "Active Directory-Benutzer und -Computer", aktivieren die "Erweiterte Features" unter "Ansicht" und wechseln in die Eigenschaften Ihres BitLocker-Clients. Hier suchen Sie innerhalb des Attribut-Editors nach dem Attribut "msTPM-OwnerInformation". Dort sollten nun die TPM-Informationen in Hash-Form hinterlegt sein.

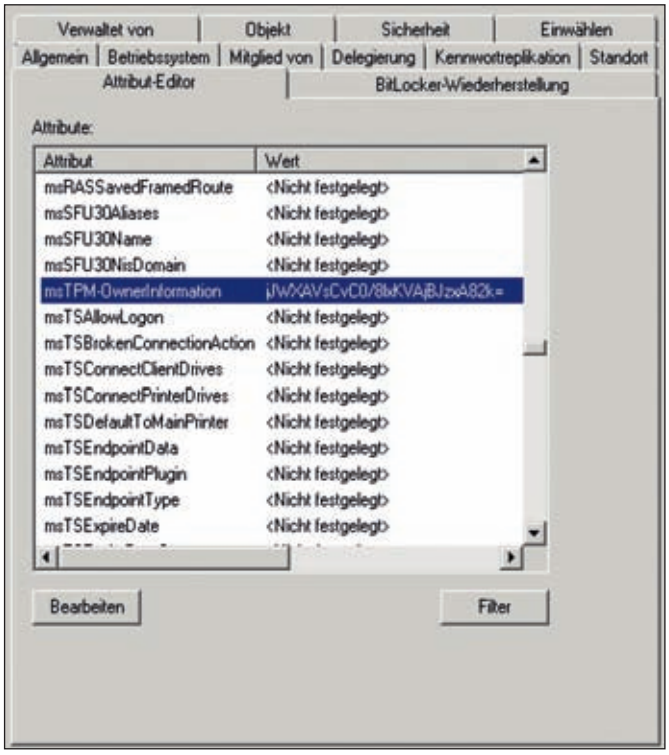


Bild 2: Ist die TPM-Information als Hash in "ms-TPM-OwnerInformation" hinterlegt, war die Zuweisung des Besitzers erfolgreich

Schritt 3: BitLocker-Gruppenrichtlinie konfigurieren

Funktioniert die eigentliche TPM-Sicherung im Active Directory, fahren Sie mit dem nächsten Schritt, der Konfiguration der eigentlichen BitLocker-Gruppenrichtlinie, fort. Hierzu öffnen Sie das bestehende Gruppenrichtlinienobjekt und wechseln in folgenden Konfigurationspfad: "Computerkonfiguration / Administrative Vorlagen / Windows-Komponenten / BitLocker-Laufwerkverschlüsselung". An dieser Stelle des Gruppenrichtlinienobjekts legen Sie nun die grundlegenden Einstellungen zur Sicherung der BitLocker-Informationen im Active Directory fest.

Diese Richtlinieneinstellung ermöglicht das Speichern von Wiederherstellungsinformationen zur BitLocker-Laufwerkverschlüsselung. Neben den benötigten Standardeinstellungen definieren Sie an dieser Stelle zudem die Option, dass der Arbeitsspeicher bei einem Neustart gelöscht und so der BitLocker-Schlüssel aus dem RAM entfernt wird. Mit dieser Richtlinieneinstellung könnte zwar die Leistung beim Neustart des Computers optimiert werden, wobei jedoch die Gefahr besteht, dass BitLocker-Schlüssel durch einen Angriff auf den Arbeitsspeicher missbraucht werden können. Im zweiten Schritt konfigurieren Sie im folgenden Pfad nun die Einstellungen für die Verschlüsselung der Betriebssystempartition: "Computerkonfiguration / Administrative Vorlagen / Windows-Komponenten / BitLocker-Laufwerkverschlüsselung / Betriebssystemlaufwerke".

Mit der Aktivierung dieser Richtlinieneinstellung konfigurieren Sie nun, dass BitLocker bei jedem Systemstart eine zusätzliche Authentifizierung erfordert. In unserem Beispiel entscheiden wir uns für die zusätzliche Authentifizierung mit TPM und einer

von uns gewählten PIN. Das heißt, dass wir bei jedem Systemstart eine Pre-Boot-Authentifizierung über eine von uns zuvor gewählte PIN durchführen müssen. Des Weiteren kann das Verhalten beim Verschlüsseln von weiteren Partitionen sowie Wechseldatenträgern festgelegt werden. Die Konfiguration unterscheidet sich hierbei jedoch nicht grundlegend, so dass wir an dieser Stelle nicht näher darauf eingehen.

Schritt 4: Verschlüsseln der Betriebssystempartition

Mit der Konfiguration der Gruppenrichtlinie haben Sie die benötigten Vorbereitungen vorerst abgeschlossen. Um die Verschlüsselung sowie die Speicherung unserer Wiederherstellungsschlüssel im Active Directory zu testen, initialisieren Sie nun die Verschlüsselung der Betriebssystempartition auf Ihrem BitLocker-Client. Der Assistent prüft die benötigten Voraussetzungen und erstellt selbstständig eine etwa 100 MByte große Boot-Partition, wenn diese nicht vorab angelegt wurde. Nach Fertigstellung fordert der Assistent erneut zu einem Neustart auf. Nach erneuter Anmeldung öffnet sich der Assistent wieder und führt durch den weiteren Konfigurationsprozess. Im nächsten Schritt wählen Sie Ihre gewünschten Systemstarteinstellungen. Wie bereits erläutert entscheiden wir uns für "Bei jedem Start PIN anfordern" und vergeben die von uns gewünschte PIN im nächsten Fenster.

Nach einem weiteren Neustart und der Eingabe unserer zuvor konfigurierten PIN können wir nun mit der Verschlüsselung fortfahren. Die reine Verschlüsselungsdauer hängt hierbei maßgeblich von der Größe der zu verschlüsselnden Partition ab und kann daher mehrere Stunden in Anspruch nehmen. Auch hier prüfen wir im Anschluss an die Verschlüsselung, ob der Wiederherstellungsschlüssel korrekt in der Active Directory-Verwaltungskonsole "Benutzer und Computer" im Computer-Objekt abgelegt und gespeichert wurde. Unter dem Reiter "BitLocker-Wiederherstellung" sollte nun ein entsprechender Eintrag zu finden sein.

Recovery von BitLocker und TPM

Nachdem alle benötigten Schlüsselinformationen für BitLocker und TPM im AD DS hinterlegt sind, sollten Sie die Wiederherstellung vollumfänglich testen. Denn nur so können Sie im Ernstfall sicherstellen, dass auf wichtige Daten jederzeit zugegriffen werden kann.

Szenario 1: TPM-PIN verloren

Sollten Nutzer ihre TPM-PIN verlieren oder vergessen, so ist es dennoch möglich, das System zu starten. Grundvoraussetzung dafür ist, dass die Widerherstellungsschlüssel ordnungsgemäß im Active Directory gespeichert wurden. Alternativ kann auch mit dem zuvor ausgedruckten Wiederherstellungsschlüssel der Recovery-Prozess angestoßen werden.

Wechseln Sie nach dem Systemstart bei der Aufforderung, Ihre PIN einzugeben, mit der "ESC-Taste" in den Wiederherstellungsmodus. Anschließend werden Sie aufgefordert, Ihren Wiederherstellungsschlüssel einzugeben. Dieser kann nun beim entsprechend verantwortlichen Helpdesk erfragt werden. Hierzu benötigt dieser lediglich die angezeigte Wiederherstellungsschlüssel-ID. Mit dieser kann er wiederum – mithilfe des zuvor installierten Features "BitLocker-Wiederherstellungskennwort-Viewer für Active Directory" – die betreffenden Wiederherstellungsinformationen schnell und einfach einsehen und die benötigten Informationen telefonisch mitteilen. Anschließend startet das System ohne Eingabe der benötigten PIN. Nach erneuter Windows-Anmeldung kann die PIN innerhalb der BitLocker Verwaltung dann vom Benutzer geändert werden.

Szenario 2: Veränderungen an der Hardware-Konfiguration

Sollten Sie Änderungen an der Hardwarekonfiguration vornehmen, so empfiehlt sich vorab, die Entschlüsselung kurzfristig zu stoppen. Dies nehmen Sie innerhalb der BitLocker-Verwaltung vor. Ansonsten gestattet BitLocker beziehungsweise das TPM nicht mehr, das System zu starten, da hier ein möglicher Missbrauch erkannt wird. Die Vorgehensweise zur Wiederherstellung in diesem Fall ist nahezu identisch zur Wiederherstellung einer verlorengegangenen PIN. Wechseln Sie auch hier nach dem Systemstart bei der Aufforderung, ihre PIN einzugeben, mit der "ESC-Taste" in den Wiederherstellungsmodus und geben Sie anschließend die vom Helpdesk mitgeteilten Wiederherstellungsschlüssel ein.

Szenario 3: TPM-Besitzerkennwort ändern

Es kann auch vorkommen, dass Sie die TPM-Benutzerkennwörter zurücksetzen müssen oder das TPM deaktiviert oder neu initialisiert werden muss. Dies kann zum Beispiel dann notwendig werden, wenn ein Mitarbeiter aus dem Unterneh-

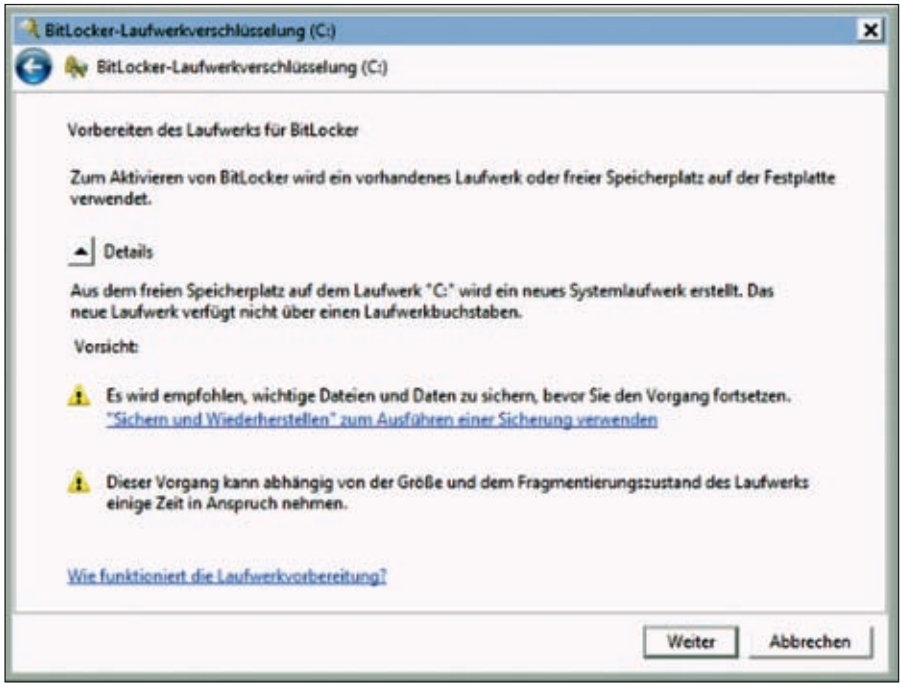


Bild 3: Nach Abschluss der Konfiguration können Sie die BitLocker-Verschlüsselung starten

men ausscheidet. Um nun das TPM-Besitzerkennwort zurückzusetzen, ist es notwendig, die entsprechende TPM-Datei zu besitzen. Ist diese aus irgendeinem Grund nicht mehr vorhanden, kann diese über die im AD DS hinterlegten und automatisch gespeicherten Hash-Werte im Computer-Attribut "msTPM-OwnerInformation" wiederhergestellt werden. Öffnen Sie hierzu einen Texteditor und fügen folgende Zeilen ein:

```
<?xml version="1.0" encoding=
  "UTF-8"?>
<ownerAuth>TPM-Hash</ownerAuth>
```

Ersetzen Sie "TPM-Hash" durch den im "msTPM-OwnerInformation"-Attribut hinterlegten Hash und speichern Sie den Schlüssel mit der Endung .tpm ab. Anschließend transferieren Sie den TPM-Schlüssel auf das Zielsystem und können das TPM-Benutzerkennwort ändern.

Anpassung des BitLocker-Kontextmenüs

BitLocker bietet zwei Verfahren zum Entschlüsseln von Datenpartitionen. Zum einen ist es möglich, beim Systemstart und der Windows-Anmeldung die verschlüsselte Partition automatisch entschlüsseln zu lassen. Oder aber die Entschlüsselung erfolgt mit einem separaten Kennwort. In der Regel empfiehlt sich die Nutzung eines separaten Kennwortes. Das einzige Problem hierbei ist, dass wenn BitLocker zur Laufzeit entschlüsselt wurde, es keine oder nur sehr eingeschränkte Built-In-Möglichkeiten gibt, diese auch wieder zur Laufzeit zu verschlüsseln.

Hintergrund ist, dass wenn Sie Ihre Datenpartition entschlüsseln und das System anschließend verlassen und sperren, der Zugriff auf sensible Daten unter gewissen Umständen möglich ist. Abhilfe schafft hier die Kommandozeile. Mithilfe des Befehls *manage-bde -lock {Laufwerksbuchstabe}* lässt sich eine entschlüsselte Partition binnen Sekunden wieder verschlüsseln. Eine bessere und elegantere Lösung hierfür ist es jedoch, das Kontextmenü von BitLocker durch einen eigenen Menüpunkt zu erweitern. Um dies auf einem BitLocker-Client zu implementieren, erstellen Sie zunächst einen Registrierungsschlüssel mit der Endung ".reg". Diese Registrierungsdatei muss folgenden Code enthalten:

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\Drive\shell\
  relock-bde]
"AppliesTo"="(System.Volume.BitLo-
  ckerProtection:=1 OR System.Volu-
  me.BitLockerProtection:=3 OR Sys-
  tem.Volume.BitLockerProtection:=5)"
@="Relock drive..."
"HasLUAShield"=""
"MultiSelectModel"="Single"

[HKEY_CLASSES_ROOT\Drive\shell\
  relock-bde\command]
@=hex(2):77,00,73,00,63,00,72,00,69,
  00,70,00,74,00,2e,00,65,00,78,00,6
  5,00,20,\

  00,6d,00,61,00,6e,00,61,00,67,00,6
  5,00,2d,00,62,00,64,00,65,00,2d,00
  ,6c,00,\

  6f,00,63,00,6b,00,2e,00,76,00,62,0
  0,73,00,20,00,25,00,31,00,00,00
```

Als Nächstes erstellen Sie eine .vbs-Datei namens *manage-bde-lock* im Ordner *System32*, die folgenden Code enthält:

```
Args = ""
Last = Wscript.Arguments.Count - 1
For i = 0 To Last
Args = Args & " " & Wscript.
  Arguments.Item(i) Next Args =
  Replace(Args,":\",":") CreateOb-
  ject("Shell.Application").Shell-
  Execute "manage-bde.exe", "-lock
  -forcedismount " & Args, "",
  "runas", 1
```

Den erstellten Registrierungsschlüssel führen Sie nun mit administrativen Rechten aus. Anschließend finden Sie im BitLocker-Kontextmenü einen weiteren Eintrag, der es Ihnen erlaubt, mit BitLocker über das Kontextmenü auch wieder zu verschlüsseln. Dieser Schritt kann auch direkt mit in den Bereitstellungsprozess über System Center Configuration Manager (SCCM) als auch über die Windows Deployment Services (WDS) einfließen.

Vereinfachte Verwaltung und Recovery mit BitLocker Administration and Monitoring

Speziell für Unternehmen, die eine Vielzahl an Windows-Systemen mit verschlüsselten Laufwerken einsetzen, ist es empfehlenswert die Microsoft BitLocker Administration and Monitoring-Tools (MBAM) zur Verwaltung einzusetzen. MBAM erleichtert dabei das Implementieren und Verwalten von Bitlocker-Laufwerken auf Systemen innerhalb des Unternehmensnetzwerkes. Dabei erleichtert ein sogenannter MBAM-Client auf den Systemen die zentrale Verwaltung. Der Client lässt sich sowohl im System Center Configuration Manager als auch über die Windows Deployment Services entsprechend für Unternehmensclients ausrollen. Systeme mit einem entsprechenden TPM-Chip können so nach der Installation die Verschlüsselung initiieren und den Benutzer im Anschluss der Installation zur Eingabe einer PIN auffordern. Zudem ermöglicht MBAM die Überwachung und Berichterstellung zum Verschlüsselungsstatus für lokale Festplattenlaufwerke und Wechseldatenträger. MBAM steht seit Anfang des Jahres allen Microsoft-Kunden mit einer Software Assurance zur Verfügung und ist Bestandteil des Microsoft Desktop Optimization Packs.

Fazit

BitLocker bietet einige Sicherheitskomponenten, die sich vor kommerziellen Lösungen nicht zu verstecken brauchen. Neben der guten Kompatibilität innerhalb einer homogenen Active Directory-Struktur bietet BitLocker im Zusammenspiel mit TPM auch einen angemessenen Schutz gegenüber den meisten Angriffsszenarien. Innerhalb großer Infrastrukturen empfiehlt sich jedoch der Einsatz der Verwaltungs- und Recovery-Funktionalitäten der MBAM-Tools. Hierdurch lässt sich sowohl die Verwaltung als auch die Wiederherstellung im Ernstfall optimieren und beschleunigen. *(dr)*

[1] BitLocker Betriebshandbuch
BBP41

Link-Codes

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

Risiken beim Einsatz von Instant Messaging und Skype

Bohrarbeiten an der Firewall


Quelle: 123RF

von Mathias Hein

Trotz der vielfach beschworenen Einheitlichkeit der Kommunikationsplattformen auf Basis von Unified Communications ist vielen Arbeitgebern der Frieden am Arbeitsplatz wichtiger als alle Sicherheitsbedenken. Aus diesem Grund werden in vielen Unternehmen auch weiterhin "störende" Anwendungen, wie beispielsweise Skype und andere öffentliche IM-Dienste, nicht von den Arbeitsplatzrechnern verbannt. Dieser Beitrag zeigt technische und rechtliche Risiken beim Einsatz von Instant-Messaging-Produkten auf und untersucht diese Risiken im Detail am Beispiel Skype.

Unified Communications (UC) beseitigt die Brüche in den Kommunikationsabläufen und somit Kommunikationshindernisse. Bestehende Anwendungen integriert UC unter einer gemeinsamen Oberfläche. Hierzu gehören beispielsweise die traditionelle Telefonie, E-Mails, Instant-Messaging- und Conferencing-Anwendungen. Neben der Integration der Kommunikationsströme – sowohl innerhalb der Unternehmen als auch hin zur Außenwelt – sorgt UC auch für die direkte Integration von Kommunikationsfunktionen in die Geschäftsanwendungen.

Fester Bestandteil fast aller kommerziellen UC-Produkte sind Instant Messaging-Funktionen. Das Instant Messaging (IM) ist ein Dienst, der es ermöglicht, mittels einer Software in Echtzeit mit anderen Teilnehmern zu kommunizieren (chatten). Dabei werden kurze Text-Mitteilungen im Push-Verfahren über ein Netzwerk (intern und extern) an den Empfänger geschickt, auf die dieser unmittelbar antworten kann. Die Integration von IM in die UC-Plattformen erweitert deren Funktionen um beispielsweise die Prüfung der Anwesenheit beziehungsweise der Verfügbarkeit von Kommunikationspartnern. Diese Funktion wird auch als Präsenzinformation bezeichnet. Steht der Partner zur Verfügung, kann sofort ein Anruf oder eine Videokonferenz über den PC aufgebaut werden. Auf diesem Weg lassen sich bei IM-Lösungen meist auch elegant Dateien austauschen. Es werden dadurch die Funktionen der klassischen Telefonie mit Echtzeit-Telediensten ergänzt.

UC kommt und IM geht … nicht

Die Einführung von Unified Communications in den Unternehmen macht natürlich auch sämtliche bisher bestehenden privaten oder proprietären IM-Lösungen obsolet. Von vielen Unternehmen werden jedoch keine strikten Maßnahmen gegen private IM-Applikationen auf den Desktops der Benutzer getroffen. Dies hat folgende Ursachen:

- Die Kunden nutzen IM-Anwendungen (beispielsweise Skype oder Google Talk) und die Sachbearbeiter wollen/müssen mit dem Kunden auf direkten Weg (Peer to Peer) kommunizieren.
- Die Nutzung öffentlicher IM-Programme durch die Mitarbeiter wird zu "privaten" Zwecken geduldet. Alle unternehmensrelevante Kommunikation erfolgt über das UC-System.
- Die Mitarbeiter nutzten IM bereits vor der Einführung von UC und bestehen weiter auf dessen Betrieb.

Durch die Nutzung nicht unternehmensgebundener Kommunikationskanäle entstehen unkontrollierte Kommunikationsebenen. Diese bedrohen das Unternehmen von der rechtlichen Seite. Wichtigstes Manko: Der Informationsaustausch, der über die proprietären/privaten IM-Zusätze am Arbeitsplatz erfolgt, wird nicht oder selten dokumentiert und nicht zentral archiviert. Damit entzieht sich diese Lösung den unternehmensüblichen Reportings und die gesetzlichen Anforderungen an die Compliance und die Kontrolle und Transparenz im Unternehmensbereich (KonTraG) werden unterlaufen.

Da die proprietären/privaten IM-Zusätze nicht in die betrieblichen Kommunikationssysteme integriert sind, werden diese auch nicht von der IT-Compliance erfasst. Wird ein solches Instant Messaging für die Übermittlung von Geschäftskorresponden-

zen verwendet oder werden per Chat wichtige Themen wie beispielsweise Auftragserteilungen besprochen, sorgt dies für einen Bruch der unternehmerischen Compliance und kann rechtliche Folgen haben.

Rechtliche Auswirkungen

Die Bedrohung leitet sich vom Begriff "Externalität" ab. Dieser beschreibt die Auswirkungen des Handelns einer Person auf eine andere. Das ökonomische Problem der externen Effekte liegt darin, dass die Verursacher der externen Effekte diese nicht im wirtschaftlichen Kalkül berücksichtigen. Ohne gesetzliche Regelungen werden im Falle negativer externer Effekte gesamtgesellschaftliche Kosten verursacht, da sie vom Entscheider nicht berücksichtigt werden, beziehungsweise im Falle positiver externer Effekte gesamtgesellschaftlicher Nutzen nicht verursacht, da der Entscheider nicht von ihnen profitieren würde. Beides ist nicht wünschenswert und führte daher zu staatlichen Regelungen. Zur Verhinderung externer Effekte hat der Staat die einschlägigen Rechtsvorschriften und auch Haftungsprinzipien erlassen.

Aus diesem Grund muss jedes Unternehmen dafür sorgen, dass mit entsprechenden technischen und organisatorischen Maßnahmen die Unternehmensressourcen vor Schaden geschützt werden, indem es den Betrieb von arbeitsfremden und somit unerwünschten Anwendungen verbietet. Die Experten sind sich einig, dass über solche privaten/proprietären Anwendungen dem Missbrauch Tür und Tor geöffnet werden. Datenklau, illegale Downloads, pornografische Daten auf Firmen-PCs, Urheberrechts- sowie Lizenzverletzungen und Datenspionage sind mögliche Folgen. Die Liste der Bedrohungen, die von solchen unerwünschten Anwendungen auf den Rechnern der Mitarbeiter ausgehen, ist für das Unternehmen und das Management nahezu endlos. Viele Manager erliegen dem fatalen Irrtum, dass sie nicht für das eventuelle Fehlverhalten ihrer Mitarbeiter oder aufgrund von Unterlassungen im Bereich der IT-Sicherheit zur Verantwortung gezogen werden können. Sind die durch mangelhafte Maßnahmen in der IT-Security entstandenen Schäden auf Managementfehler zurückzuführen, können heute die Mitglieder der Geschäftsleitung persönlich haftbar gemacht werden. Als Fehler ist bereits zu interpretieren, wenn die Sicherheit des Netzes/der Endgeräte keiner Überprüfung unterzogen wird und es somit auch nicht zur Einleitung geeigneter Abwehrmaßnahmen gegen Angriffe kommt.

Wir betrachten die IM-Problematik im Detail nun am Beispiel "Skype". Etwa zehn Prozent aller internationalen Telefonminuten wurden im vergangenen Jahr über Skype abgewickelt. Der unkontrollierte Einsatz von Skype in den Unternehmensnetzen birgt jedoch erhebliche Sicherheitsprobleme und zusätzliche Risiken für die Unternehmen.

Skype im Unternehmensnetz birgt Sicherheitsrisiken

Eine Installation von Skype erfordert keine Administrationsrechte. In der Praxis ignorieren die meisten Mitarbeiter die Sicherheitsvorgaben des Unternehmens und installieren und nutzen Skype, ohne die IT-Abteilung zu informieren. Dies hat zur Folge, dass die Unternehmen faktisch keine Kontrolle über die durch Skype übermittelten Daten haben.

Skype basiert darüber hinaus auch nicht auf einem der gängigen VoIP-Standards (SIP, H323 oder ähnlichem), sondern nutzt drei proprietäre Protokolle. Darüber hinaus arbeitet Skype als Peer-to-Peer-Technologie. Jeder Client (somit jedes Skype-Phone) verbindet sich nicht mit einem zentralen Server, sondern ohne weitere Konfiguration mit anderen Clients (Peers). Aus diesem Grund verschlüsselt Skype auch die Verbindungen. Das Skype-Protokoll nutzt zur Verschlüsselung den AES (Advanced Encryption Standard)-Mechanismus. Die symmetrischen Schlüssel werden dabei dynamisch ausgehandelt. Die benutzten Verfahren gelten als extrem sicher. Daneben betreibt Skype innerhalb seines Netzwerkes eine Public Key Infrastruktur (PKI), die Austausch und Überprüfung der Schlüssel erlaubt. Allerdings warnen Kryptografie-Experten, dass die in Skype eingebaute Verschlüsselung nicht sicher genug sei und Verbindungen mitgeschnitten und entschlüsselt werden könnten.

Um zu verhindern, dass der Skype-Verkehr extern blockiert werden kann, hat Skype sehr viel Aufwand in die Verschleierung der eigenen Datenströme investiert. Wird eine Skype-Verbindungsmethode unterbunden, greift das Programm auf eine Vielzahl von Fallback-Mechanismen zurück, die es systematisch durchprobiert. Skype-Datenströme werden beispielsweise auch als getarnter Webverkehr oder HTTPS übertragen.

Die Umgehung der Sicherheitsfunktionen durch Skype bereitet den IT-Administratoren einiges Kopfzerbrechen. Skype legt beispielsweise nach dem Start im Verzeichnis für temporäre Dateien die ausführbare Datei *1.com* an. Diese ist in der Lage, sämtliche BIOS-Informationen des betreffenden Rechners auszulesen. Darüber hinaus versucht Skype das Auslesen dieser Datei zu unterbinden. Nach Aussage von Skype diene diese Überprüfung dem "Skype Extras Manager" zur eindeutigen Identifizierung von Rechnern, damit sichergestellt werde, dass lizenzpflichtige Extras nur von berechtigten Lizenznehmern installiert und betrieben werden.

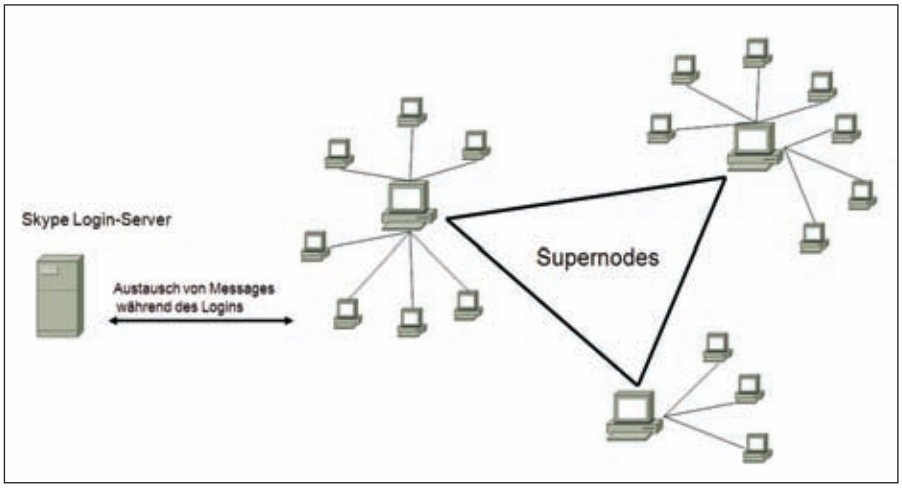


Bild 1: Die Architektur des Skype-Netzwerks mit zentralem Login-Server und Supernodes

Sicherheitskritische Aspekte der Skype-Architektur

Auf Basis von Skype ist es möglich, auch zwischen Clients, die durch eine Firewall geschützt sind, VoIP-Verbindungen herzustellen. Möchte Nutzer A mit Nutzer B sprechen und sind beide durch eine Firewall geschützt, sind in keiner Richtung eingehende Verbindungen möglich. Befindet sich jedoch nur Nutzer A hinter einer Firewall, kann Nutzer A den Nutzer B anrufen, aber nicht B den Benutzer A. Jeder Skype-Client ist mit einem Supernode verbunden, der letztlich als Verteiler agiert. Dabei kann jeder Skype-Client als Supernode arbeiten. Somit sind Supernodes keine zentralen Server, sondern andere Skype-Nutzer. Dem IT-Administrator wird durch dieses Prinzip allerdings die Kontrolle entzogen.

Beim Verbindungsaufbau (Bild 2) wird über eine bereits bestehende Verbindung zum Supernode (C) auf Basis des "Skype Proprietary Call Control Protocols" ein eingehender Anruf signalisiert. Anschließend verbinden sich A und B mit dem Supernode C und bauen über Rechner C das Gespräch auf. Das eigentliche Gespräch wird anschließend direkt zwischen A und B (per UDP-Verbindung) abgewickelt.

Erlaubt eine sehr restriktiv konfigurierte Firewall den Transfer des ausgehenden Datenverkehrs nur über die TCP-Ports 80 (HTTP) und 443 (HTTPS) und sind die UDP-Wege blockiert, wird das Gespräch über andere Computer (D) geführt. Diese Funktion wird als Relaying bezeichnet und lässt sich nicht nur für die Übermittlung von Sprache, sondern auch zur Datenübertragung nutzen. Die Transferrate einer solchen Verbindung ist nicht sehr hoch, aber immerhin kommt die Dateiübertragung überhaupt zustande.

Ein Mechanismus zur Durchdringung von Firewalls wird als "UDP Hole Punching" bezeichnet. Normalerweise können zwei Rechner, die sich beide hinter einer Firewall befinden, keine direkte Kommunikation aufbauen. Rechner hinter einer Firewall sind durch Network Address Translation (NAT) aus dem Internet nicht direkt adressierbar. Selbst wenn die übersetzte IP-Adresse eines solchen Rechners

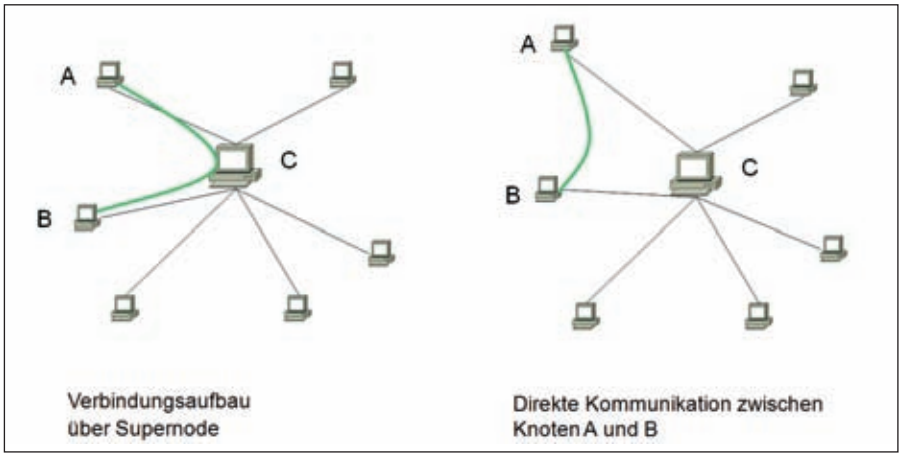


Bild 2: Im Skype-Netzwerk erfolgt der Verbindungsaufbau entweder Peer-to-Peer oder über Supernodes

bekannt ist und versucht wird, über diese zu kommunizieren, wird die Firewall der Gegenseite die Kommunikation unterbinden, weil diese nicht von ihrem Netz aus aufgebaut wurde.

Beim UDP Hole Punching wird mit Hilfe eines externen Vermittlungsservers trotzdem eine Kommunikation ermöglicht. Clients, die kommunikationsbereit sind, melden sich bei diesem externen Server an. Dadurch ist der Firewall bekannt, dass sie auch Pakete von diesem externen Server als Antwort durchlassen muss. Die Kommunikation der beiden Clients untereinander läuft dann jeweils über den Server, der die Pakete mit seiner Adresse als Absender weiterleitet. Das UDP Hole Punching macht es sehr schwer, Skype beispielsweise in Firmennetzen zu blockieren. Durch die Möglichkeit, Dateien über Skype zu übertragen, ist Skype die perfekte Methode, um unerkannt Daten aus abgesicherten Bereichen zu schmuggeln.

Ressourcenfresser Supernode

Die Registrierung als Skype-Nutzer und die Installation der Software erkauft der Anwender mit der Bereitstellung der Ressourcen des eigenen Computers beziehungsweise des Firmenrechners für die Skype-Community. Besitzt der als Skype-Client verwendete Rechner die richtigen Voraussetzungen – lange Online-Zeiten, hohe Bandbreite, eine öffentliche IP-Adresse, reichlich Rechenpower und Arbeitsspeicher –, kann dieser zu einem Supernode mutieren und damit zu einer Vermittlungszentrale für Adressbücher, Presence-Informationen und die Kommunikationsströme der Skype-User werden.

Mit dem Befehl *netstat* lässt sich feststellen, ob der eigene Computer als Supernode agiert. Tauchen in den Statistiken über einen längeren Zeitraum viele unbekannte Verbindungen auf dem in den Skype-Optionen unter "Connection" festgelegten Port auf, ist dies wohl ein gewisses Indiz für einen Supernode. Es kann aber genauso sein, dass der eigene Computer "nur" zum Relaying verwendet wird. Tatsächlich hat ein Supernode viele neue eingehende Verbindungen, die Sie allerdings durch einmaligen netstat-Check nicht unbedingt erkennen. Daher sollten Sie die eingehenden Verbindungen über einen längeren Zeitraum beobachten. Außerdem erzeugt ein Supernode ein deutlich höheres Datenvolumen als normale Knoten.

Es besteht kein Zusammenhang zwischen einer großen Anzahl an Verbindungen und dem Status als Supernode. Um den Status eines Supernodes zu erhalten, benötigt der Rechner eine schnelle Internet-Anbindung, der in Skype festgelegte Port darf für eingehende TCP- und UDP-Verbindungen nicht durch eine Firewall blockiert sein und Skype muss tage- beziehungsweise wochenlang ohne Neustart laufen. Supernodes werden automatisch ausgewählt und bei einer Überlastung gibt Skype einen Teil der Last an einen der verbundenen Clients ab (die Last wird automatisch verteilt). Ein Supernode stellt von sich aus Bandbreite zur Verfügung, über die der Benutzer in einem Unternehmensnetz keine Verfügungsgewalt hat. Ab Version 3.0 des Skype-Clients lässt sich

diese Funktionalität über Registry-Keys ausschalten. Auf allen Rechnern, deren Verfügbarkeit garantiert werden muss, sollte die Funktionalität als Supernode oder Relay bei der Installation des Skype-Client ausgeschaltet werden. Voraussetzung dafür ist jedoch, dass Mitarbeiter Skype nicht unkontrolliert ins Unternehmen einführen.

Skype macht das eigene Netzwerk angreifbar

Ein wesentlicher Sicherheitsaspekt ist die Gefahr, dass über Skype-Verbindungen das eigene Netzwerk angreifbar wird. Skype betreibt einen immensen Aufwand, um das Reverse Engineering seiner Software zu verhindern. So erkennt der Client beispielsweise, ob er in einem Debugger läuft und ändert sein Laufzeitverhalten, indem er andere Register und Speicherbereiche nutzt. Teile des Codes sind sogar verschlüsselt und werden erst zur Laufzeit ausgepackt. Darüber hinaus ist es den Systementwicklern gelungen, die Art der Datenverschlüsselung, die Berechnung des Schlüssels sowie die Authentifizierung von Skype herauszufinden. Prinzipiell besteht so die Möglichkeit, manipulierte Supernodes ins Netz zu bringen, um den Sprachverkehr umzuleiten und zu belauschen.

Durch die fehlende Transparenz von Skype ist die Applikation oft nicht mit der Sicherheitspolitik eines Unternehmens vereinbar. So können eventuell schon vorhandene oder zukünftige Backdoors nicht erkannt werden. Das Netzwerk ist gegen Angriffe ungeschützt, da die Angriffe über Skype grundsätzlich versteckt sind. Weiterhin wird ein Datenverkehr erzeugt, den IT-Verantwortliche nicht einfach überwachen können. Jeder Nutzer von Skype muss automatisch nicht nur den anderen Nutzern, sondern auch jeglichen Knoten, die für die Verbindungen genutzt werden, blind vertrauen. Auch wenn die Entwickler von Skype alles daransetzen, eventuelle Sicherheitslücken zu schließen, treten wie bei allen Softwareentwicklungen derartige Lücken immer wieder auf. Da eine Skype-Verbindung quasi einen Tunnel durch die Firewall eines Netzwerkes aufbaut, ist die Gefahr, dass Dritte über eine solche Verbindung unberechtigt eindringen, gegeben. Und anders als bei reinen Telefonverbindungen ist damit der Zugriff auf sämtliche Daten im Netzwerk, das Einschleusen von Trojanern und Spyware oder die Verseuchung mit einem Virus möglich.

Außerdem baut Skype sehr viele Internetverbindungen auf, welche das Intrusion Detection System (IDS) nicht eindeutig zuordnen kann und führt gleichzeitig zu einer erhöhten Rate von fehlerhaften Sicherheitsalarmen. Dies zieht einerseits das Risiko nach sich, dass wichtige Alarme zwischen Fehlalarmen übersehen werden. Andererseits würden zu lockere Sicherheitseinstellungen für IDS ein größeres Risiko darstellen, da tatsächliche Angriffe nicht erkannt werden.

Der Einsatz von Skype in den Unternehmen lässt sich mit gängigen Maßnahmen kaum blockieren. Jeder Skype-Client verwendet einen anderen Port. Dieser Kommunikationsport wird bei der Installation nach dem Zufallsprinzip festgelegt. Aus diesem Grund lässt sich der Skype-Verkehr nicht ohne weiteres in der Firewall, etwa durch die Blockierung einzelner Ports, unterbinden.

Zudem basiert Skype auf einer Peer-to-Peer-Technologie und daher kann kein zentraler Server blockiert werden. Bleibt noch der Login-Server, auf dem sich jeder Nutzer anmelden muss, um einen neuen Account zu registrieren und um sich im Skype-Netzwerk anzumelden, falls er nicht die Option Autologin aktiviert hat. Hat sich ein Nutzer bereits angemeldet (möglicherweise von zu Hause) und wurde die Option Autologin gewählt, braucht der Benutzer nicht einmal mehr eine Verbindung zu einem Login-Server. Die Login-Server verfügen über feste IP-Adressen (beispielsweise 80.160.91.5, 80.160.91.11, 80.160.91.13, 80.160.91.25). Daher könnte der Zugriff auf diese Server blockiert werden. Dies bietet jedoch keinen hundertprozentigen Schutz.

Risiken durch Skype

Die Installation und der Betrieb von illegalen Kommunikationskanälen sind durch Mitarbeiter technisch vergleichsweise leicht zu bewerkstelligen. Dies fällt den Mitarbeitern umso leichter, wenn das Unternehmen nur mittelmäßige Sicherheitsmaßnahmen etabliert und diese zudem nicht speziell auf Skype abgestimmt hat.

Die größte Gefahr beim Einsatz von Skype geht vom Risiko des Datenabflusses aus. Mit anderen Worten: Durch Skype können vertrauliche Unternehmensdaten unbemerkt aus dem Unternehmen hinaus geschmuggelt werden. Der Missbrauch von Arbeitszeit, Speicherplatz und Bandbreite kann zwar zu erheblichen arbeitsrechtlichen Konsequenzen für die Mitarbeiter bis hin zur fristlosen Entlassung führen – für das Unternehmen ist dies aber nur eine relativ unbefriedigende Begrenzung eines Schadens, der in der Regel schon längst entstanden ist.

Unternehmen, deren Mitarbeiter durch unbemerkt und unkontrolliert laufende Plattformen Urheberrechte verletzen, können dafür samt ihrer Vorstände und Geschäftsführer zur Rechenschaft gezogen werden. Die rechtlichen Konsequenzen reichen dabei von Unterlassungs- und Schadensersatzansprüchen bis hin zu Haftstrafen für die Geschäftsführung.

Fazit

In den Unternehmen werden die IM-Vorteile ausgiebig genutzt. Aus diesem Grund muss deren Nutzung in die täglichen Geschäftsabläufe eingebunden werden. Die konsequente Beseitigung der proprietären/privaten IM-Anwendungen auf den Desktops der Nutzer trägt deutlich zur Absicherung der Unternehmen und zur Rechtssicherheit bei.

Skype sollte in Unternehmen und vor allem in Bereichen, in denen mit geheimen Informationen gearbeitet wird, nicht eingesetzt werden. Das bedeutet jedoch nicht, dass die Nutzung von Skype in Unternehmen generell ausgeschlossen werden sollte. Der Einsatz muss jedoch unter Beachtung klar definierter Regeln erfolgen. Dazu gehört auch, dass Mitarbeiter über die Risiken von Skype informiert und für den Umgang mit unternehmenskritischen Daten sensibilisiert werden. Denn IT-Sicherheit entsteht nicht nur durch technische Schutzmaßnahmen. Ein mindestens ebenso wichtiger Faktor ist ein gesundes Maß an Misstrauen und Wachsamkeit gegenüber der Software, die auf den Systemen läuft. *(jp)*

PowerShell 2.0

Schnellstartleiste für Windows 7

von Rolf Masuch

Bei der Anpassung der Windows 7-Taskleiste mittels VBS-Skript gibt es zwei Herausforderungen: Die Erste ist die jeweilige Sprache, in der das Betriebssystem installiert ist. Das Kontextmenü wird natürlich in der für den Benutzer gewählten Sprache angezeigt. Dies mag jetzt nicht für alle Windows-Nutzer ein Thema sein. Doch der zweite Teil betrifft alle Sprachen und die – leider nicht sofort sichtbaren – Tastaturkürzel zur Anwahl einzelner Menüpunkte. Sie machen diese sichtbar, indem Sie zuerst die STRG-Taste drücken und dann das Kontextmenü aufrufen.

In einem TechNet-Artikel [1] zu diesem Thema wird zunächst ein Ordnerobjekt aus der entsprechenden Verknüpfung heraus erzeugt. Wichtig ist dabei, dass es sich ausdrücklich nicht um ein Dateiobjekt handeln darf. Nun werden die Kommandoverben des Objektes ermittelt und in einer Sammlung von Zeichenketten gespeichert. In Schritt drei wird jede Zeichenkette einzeln analysiert. In diesem Analyseschritt wird das "&" jeweils entfernt. Dieses verwenden Programmierer, um eben genau die Tastaturkürzel zu erzeugen. Und erst wenn die bereinigte mit der gewünschten Zeichenkette übereinstimmt, kommt im letzten Schritt das Kommando "Doit" in Bezug auf das Kommandoverb selbst zum Einsatz (Kasten "Pin to Taskbar mit VBS").

Doch das VBS-Skript deckt noch eine weitere Schwäche dieses Ansatzes auf: Es ist zu unflexibel und kann nur mühsam parametrisiert werden. Wenn Sie jedoch die PowerShell nutzen, um dieses Problem zu lösen, können Sie auf die Flexibilität der Sprache zurückgreifen, um das Skript universeller einzusetzen. Es sollten dabei die Aktionen "Pin" und "Unpin" sowie "CurrentUser" oder "AllUser" unterstützt werden.

Der Ablauf ist im PowerShell-Skript identisch zum VBS-Skript. Nur ist hier der Aufbau in Form einer einfachen Funktion gestaltet. Dadurch lassen sich Redundanzen im Code vermeiden und die einmalig ermittelten Ordner können mehrfach verwendet werden. Der Hauptteil der Arbeit wird im Block "Process" getan. Nach ein paar Logikprüfungen wenden wir die identische Vorgehensweise wie im VBS-Skript an, um die Verben zu ermitteln, dann das "&" zu entfernen und die lokalisierte Zeichenkette mit dem Ergebnis zu vergleichen. Auch hier wenden wir den Befehl "Doit" auf dieses gefundene Kommando an. Offen bleibt aber die Anpassung an die jeweilige Sprache des installierten Systems. Hierzu findet sich im Skript Repository ein PowerShell-Modul [2], das auch noch dieses Thema adressiert. Damit wird dann auch noch das Startmenü ansprechbar. *(dr)*

```
Const CSIDL_COMMON_PROGRAMS = &H17
Const CSIDL_PROGRAMS = &H2
Set objShell = CreateObject("Shell.Application")
Set objAllUsersProgramsFolder = objShell.
   NameSpace(CSIDL_COMMON_PROGRAMS)
strAllUsersProgramsPath = objAllUsersPrograms
   Folder.Self.Path
Set objFolder = objShell.Namespace(strAllUsers
   ProgramsPath & "\Accessories")
Set objFolderItem = objFolder.ParseName
   ("Calculator.lnk")
Set colVerbs = objFolderItem.Verbs
For Each objVerb in colVerbs
    If Replace(objVerb.name, "&", "") = "Pin to
   Start Menu" Then objVerb.DoIt
Next
```

Listing: Pin to Taskbar mit VBS

[1] Technet VBS Artikel zur Taskleiste
BAPF1

[2] PowerShell Modul zum Modifizieren der Taskbar und des Startmenüs
BAPF2

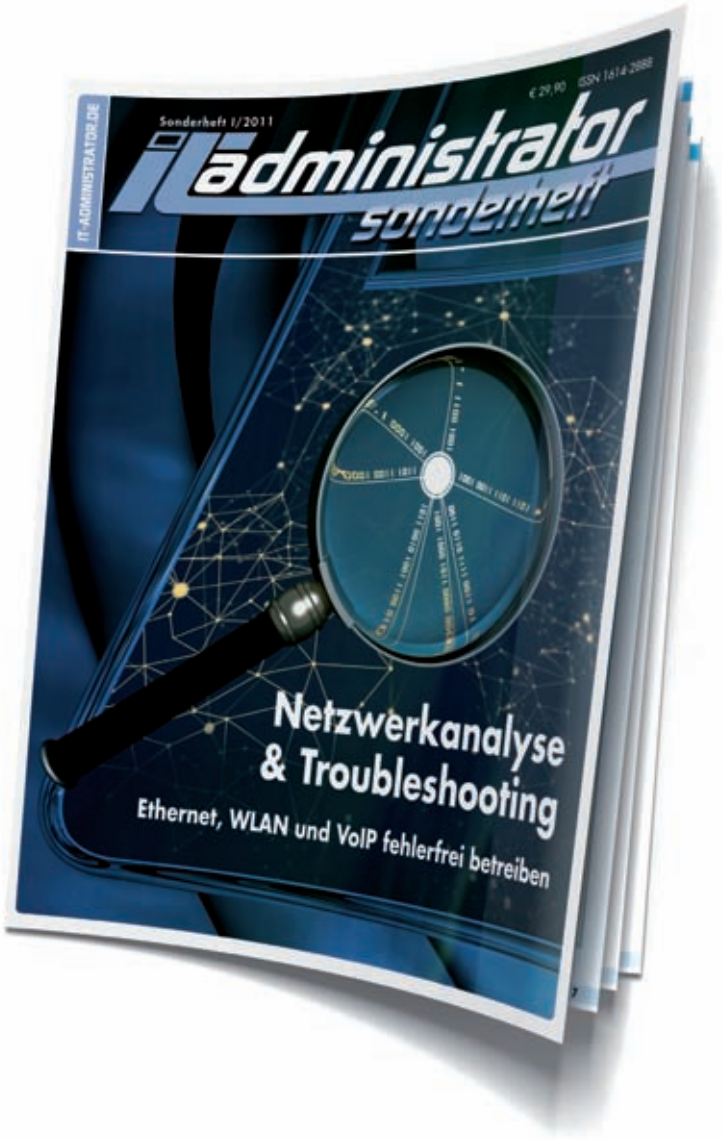
Link-Codes

```
function Set-PinnedElement
{
param(
[string] $element,
[string] $action,
[string] $scope,
[string] $subdir
)
begin {
    $shell = new-object -ComObject Shell.Application
    $CurrentUserStartFolderPath = "$env:APPDATA\
            Microsoft\Windows\Start Menu\Programs\"
    $AllUsersStartFolderPath = "$env:ALLUSERSPROFILE\
            Microsoft\Windows\Start Menu\Programs\"
}
process {
    if ($_){$element = $_}
   switch ($scope) {
            "CurrentUser" {$workdir = $CurrentUser
            StartFolderPath}
            "AllUsers" {$workdir = $AllUsersStart-
            FolderPath}
            "custom" {$workdir = $subdir}
            default {$workdir = $CurrentUserStart-
            FolderPath}
   }
   if (($subdir) -and ($scope -ne "custom")) {$workdir
   = "$workdir$subdir\"}
   elseif (($subdir) -and ($scope -eq "custom"))
   {$workdir = "$subdir\"}
   if (test-path -Path "$workdir$element.lnk") {
        $Folder = $shell.NameSpace($workdir)
        $FolderItem =
   $Folder.ParseName("$element.lnk")
        $verbs = $FolderItem.Verbs()

        switch ($action){
        "add" {
            ForEach ($verb in $verbs){if (($verb.Name
   -replace "&", "") -eq "An Taskleiste anheften"){
                $verb.DoIt();write "$element added to
                taskbar"}}}
        "remove" {
            ForEach ($verb in $verbs){if (($verb.Name
             -replace "&", "") -eq "Von Taskleiste
             lösen"){$verb.DoIt();write "$element
             removed from taskbar"}}}
        }
    }else{write "$element not found"}
}
end{}
}
#Beispielaufrufe
#Set-PinnedElement "Internet Explorer" -action Add
#Set-PinnedElement "Internet Explorer" -action Add
   -scope CurrentUser
#Set-PinnedElement "File Transfer Manager" -action Add
   -scope custom -subdir "C:\Users\Rolf\desktop"
#Set-PinnedElement "Mozilla Firefox" -action Add
   -scope AllUsers -subdir "Mozilla Firefox"

#Set-PinnedElement "Internet Explorer" -action Remove
#Set-PinnedElement "Mozilla Firefox" -action Remove
   -scope AllUsers -subdir "Mozilla Firefox"
#Set-PinnedElement "File Transfer Manager" -action Re-
   move -scope custom -subdir "C:\Users\Rolf\desktop"
```

Listing: Pin/Unpin to Taskbar via PowerShell



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. 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 1211

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

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

Der **Virtual Machine Manager 2012** steht bisher ja **nur als Release Candidate** zur Verfügung. Da ich als Administrator von Hyper-V schon sehr gespannt auf diesen Bestandteil des System Center bin, würde ich die neueste Version gerne schon jetzt einmal unter Laborbedingungen ausprobieren. Doch **wie führe ich das Upgrade auf die kommende Version** am besten durch?

Für den Einsatz von SCVMM 2012 existieren zwei Möglichkeiten: Ein In-Place-Upgrade oder die Neuinstallation des Release Candidate beziehungsweise später der RTM-Version. Damit Sie eine bestehende Konfiguration und deren Daten (VM-Hosts, Virtual Machines Templates et cetera) übernehmen können, bietet sich ein In-Place-Upgrade an. Dabei werden die VMM-Datenbank, die VMM-Serverkomponenten sowie die VMM-Agenten der VM-Hosts aktualisiert. Vor dem Upgrade sollten Sie auf jeden Fall ein Backup der VMM 2008 R2 Database anfertigen. Damit stellen Sie sicher, dass Sie bei einem Fehlschlag des Upgrades jederzeit auf die Vorgängerversion zurückgehen können. Während des Umstiegs auf SCVMM 2012 müssen Sie weiterhin den VMM Service Account und das gewünschte Encryption Management konfigurieren. Ratsam ist hier in der Regel ein dedizierter VMM Service Account sowie der Einsatz von Distributed Key Management (DKM). Im Internet (Link-Code BBPE5) finden Sie detailliertere Informationen zu DKM. Haben Sie bereits bei SCVMM 2008 R2 einen Service Account eingesetzt, so müssen Sie bei SCVMM 2012 das gleiche Konto verwenden. Während des Upgrade-Prozesses ist es erforderlich, das entsprechende Passwort einzugeben, das Sie also zur Hand haben sollten. Nachdem Sie sämtliche Vorbereitungen getroffen haben, geht es nun zum eigentlichen Upgrade. Schließen Sie zuallererst sämtliche Verbindungen auf den VMM-Server. Dies beinhaltet auch die VMM-Administrationskonsole, die VMM Command Shell sowie das VMM Self-Service Portal. Sofern sich die VMM-Datenbank bereits auf einem SQL Server befindet, ist der In-Place-Upgrade auf SCVMM 2012 sehr einfach durchzuführen. Die Setup-Routine erkennt, dass sich bereits eine ältere Version auf dem Server befindet – daher können auch nur wenige Optionen selektiert beziehungsweise konfiguriert werden. Einzig WAIK 1.0 müssen Sie manuell deinstallieren und WAIK 2.0 aufspielen. Für den Fall, dass Sie für die VMM-Datenbank bei der ursprünglichen Installation die SQL Express-Variante gewählt haben, müssen Sie vor dem In-Place-Upgrade noch die VMM-Datenbank migrieren. Dies ist ein klein wenig aufwändiger, aber noch immer mit relativ wenig Mühe durchzuführen. Dazu gilt es folgende Schritte zu beachten: Stoßen Sie auf jeden Fall ein Backup der Datenbank an und stellen Sie die VMM Database auf dem neuen SQL-Server wieder her. Tragen Sie dann den VMM Service Account als "dbo" ein. Auf dem VMM Server deinstallieren Sie jetzt WAIK 1.0 und spielen WAIK 2.0 auf. Konfigurieren Sie dann einen entsprechenden VMM Service Account und greifen Sie auf Distributed Key Management zurück. Nachdem die Installation des VMM-Servers abgeschlossen ist, müssen Sie noch die VMM-Agenten der VM-Hosts, die mit VMM verwaltet werden, sowie auch den VMM Library Server auf die aktuelle Version aktualisieren. Unter der Option "Fabric / Servers" erhalten Sie einen Gesamtüberblick. Dort wählen Sie sämtliche Computer mit dem Status "Upgrade Available" aus und bringen Sie mit "Update Agent" auf den aktuellen Stand. In der Regel müssen die Agenten jedoch nicht sofort aktualisiert werden, denn SCVMM 2012 arbeitet (mit wenigen Einschränkungen) auch mit älteren Versionen zusammen.

(Michel Lüscher/ln)

Server Talk

Weitere Informationen zu Server 2008 R2 und Hyper-V finden Sie auf www.server-talk.eu

RDP-Verbindungen greifen ja über **Port 3389** auf den Rechner zu. Aus Sicherheitsgründen würden wir unseren Windows-Clients gerne **einen anderen Port zur Nutzung von RDP zuweisen**. Wie kann ich die entsprechenden Settings am schnellsten und einfachsten umstellen?

Eine Änderung des Standard-Ports für den RDP-Zugriff erreichen Sie am schnellsten über die Registry. Nachdem Sie diese mit *regedit* gestartet haben, navigieren Sie zum Eintrag "HKEY_LOCAL_MACHINE / SYSTEM / CurrentControlSet / Control /

Der Standard-Port für den RDP-Zugriff lässt sich über die Windows-Registry leicht ändern

Terminal Server / WinStations / RDP-Tcp". Klicken Sie nun mit der rechten Maustaste auf den Schlüssel "PortNumber" (DWORD) und wählen Sie die Option "Ändern". Setzen Sie die Basis für den Wert auf "Dezimal" und tragen Sie den gewünschten Port ein, der zwischen 1025 und 65.535 liegen muss. Klicken Sie dann auf "OK" und führen Sie einen Neustart des Systems durch. In Zukunft funktioniert der RDP-Zugriff nur noch über den neu eingestellten Port. *(ln)*

Seit Windows Vista ist auf dem Betriebssystem aus dem Hause Microsoft standardmäßig **kein Telnet-Client** mehr installiert. Dies lässt sich nur über die Systemsteuerung nachholen, was ich allerdings als äußerst unpraktisch empfinde, wenn ich gerade mitten in der Kommandozeileneingabe stecke. Gibt es denn keine **Möglichkeit, um Telnet mit einem schlanken Befehl zu installieren?**

Wie Sie schon richtig vermutet haben, gibt es eine Möglichkeit, den Telnet-Client über die Kommandozeile auf den Rechner zu bringen. Geben Sie dazu einfach den folgenden Befehl ein:

```
dism /online /Enable-Feature
  /FeatureName:TelnetClient
```

Das Praktische an dieser Zeichenfolge ist, dass Sie unmittelbar nach dem Durchlaufen des Kommandos in der Befehlszeile mit Telnet arbeiten können. *(ln)*

Viele weitere Tipps & Tricks sowie konkrete Hilfe bei akuten Problemen bekommen Sie auch im Internet bei unserem exklusiven Foren-Partner administrator.de. Über 60.000 registrierte Benutzer tauschen dort in über 100 Kategorien ihre Erfahrungen aus und leisten Hilfestellung. So wie der IT-Administrator das praxisnahe Fachmagazin für Administratoren ist administrator.de die Internetplattform für alle System- und Netzwerkadministratoren.
www.administrator.de
ADMINISTRATOR | IT-FORUM

Auf einigen unserer mobilen Rechner nutzen wir **Microsofts Security Essentials**. Trotz der gelungenen Installation **startet der Dienst nicht** – auf dem Bildschirm erscheint stattdessen folgende Fehlermeldung: "Der Computer wird nicht von Microsoft Security Essentials überwacht, da der Dienst des Programms angehalten wurde. Sie sollten ihn jetzt neu starten." Wo liegt hier das Problem?

Die Schwierigkeiten beim Start der für die Security Essentials benötigten Dienste können viele Gründe haben. Zum einen kommt das Werkzeug oft mit Sicherheits-Tools von Drittanbietern in Konflikt. Überprüfen Sie deshalb über die Systemsteuerung beziehungsweise den Befehl *appwiz.cpl*, ob ein anderer Malware- und Spam-Schutz auf dem Rechner installiert ist. Ist dies der Fall, deinstallieren Sie ihn. Öffnen Sie nun über das Suchfeld beziehungsweise die Schaltfläche "Ausführen" und den Befehl *services.msc* die Liste mit den installierten Diensten. Suchen Sie den Dienst "Microsoft Anti-Malware-Dienst" und gehen Sie mittels der rechten Maustaste auf die Option "Eigenschaften". Überprüfen Sie, ob als "Starttyp" auch wirklich "automatisch" festgelegt ist. Läuft der Dienst nicht bereits, klicken Sie auf "Starten". Wenn die Schaltfläche "Starten" nicht verfügbar ist, klicken Sie auf die Schaltfläche "Beenden" und versuchen Sie noch einmal, den Dienst neu zu initiieren. Fruchtet dies alles nichts, sollten Sie Microsoft Security Essentials deinstallieren und neu installieren. Treten bei der automatischen Deinstallation über die Systemsteuerung Fehler auf, hilft Ihnen ein Eintrag auf den Support-Seiten von Microsoft weiter (*Link-Code* BBPE6). *(ln)*

vmware®

Auf der **VMware-Webseite** möchten wir uns diverse **Datacenter-Produkte herunterladen**. Leider tauchen dabei immer wieder Probleme auf. Entweder lässt sich überhaupt kein Download initiieren oder aber dieser **bricht unmittelbar nach dem Beginn mit folgender Meldung ab** "Sorry, at the moment you are not authorized to download {Name des VMware-Produkts}". Passende Lizenzen sind eigentlich vorhanden. Was ist hier also zu tun?

Sie können VMware Datacenter-Produkte nur dann herunterladen, wenn Sie entweder der primäre oder der sekundäre Lizenzadministrator oder der Support-Administrator für die in Ihrem Konto registrierten Lizenzen des oder der Produkte sind, das / die Sie herunterladen wollen. Eine Ausnahme bildet der VMware vCenter Converter, der frei verfügbar ist. Um etwaige Probleme zu beheben, stellen Sie also zunächst sicher, dass Sie eine der oben genannten Administratoren-Rollen haben beziehungsweise erhalten. Nähere Informationen zu diesem Thema und zu den generellen Unterschieden der einzelnen Admin-Rollen erhalten Sie im Internet (*Link-Codes* BBPE7 und BBPE8). Wenn Sie im Besitz der erforderlichen Berechtigungen sind, können Sie über http://vmware.com/download/ unter dem Punkt "Datacenter Downloads and Desktop Downloads" das Herunterladen verfügbarer Produkte starten. Beachten Sie, dass Sie über die Option "View History" eine ältere Version oder ein Update des Produkts auswählen können. In der Login-Anzeige geben Sie nun Ihre registrierte E-Mailadresse und Ihr Passwort für die Anmeldung ein. Sind diese korrekt beziehungsweise verfügen Sie über die erforderlichen Berechtigungen, sehen Sie nun die entsprechenden Binaries. Für die Übertragung können Sie entweder auf den Download-Manager oder den Webbrowser zurückgreifen. Um Probleme oder Fehler zu beheben, die bei der Nutzung des Download Managers auftreten, sehen Sie sich im Web zwei FAQs an (*Link-Codes* BBPE9 und BBPE0). Sollten dann immer noch Probleme auftauchen, löschen Sie sämtliche Cookies und temporäre Dateien Ihres Browsers. Gegebenenfalls sollten Sie versuchen, mit einem komplett anderen Browser auf die Download-Seite zuzugreifen. *(VMware/ln)*

CITRIX

Seit dem **Update auf den Internet Explorer 9** können Anwender nach dem Einloggen in das **Citrix Web Interface keine Anwendungen mehr starten**. Stattdessen erscheint eine Meldung, ob die Datei *launch.ica* geöffnet werden soll. Die Anwendung startet jedoch nicht. Wie lässt sich dieses Problem aus der Welt schaffen?

Der Fehler wird durch das veränderte Download-Verhalten des neuen Internet Explorers verursacht. In der aktuellen Version des Citrix Online Plugins (ab Version 12.1.44) ist dieser Fehler bereits behoben. Alternativ lässt sich das Problem aber auch durch folgende Einstellungen umgehen: Deaktivieren Sie zunächst den ActiveX-Filter. Klicken Sie dazu das Menü "Einstellungen" (Rädchen-Icon oben rechts im Browser-Fenster) an. In der Dropdown-Liste wählen Sie den Menüpunkt "Sicherheit / Safety" aus und deaktivieren dort die ActiveX-Filterung. Um im Anschluss daran den Start des ICA-Objekts zu erlauben, gibt es zwei Möglichkeiten: Unter "Internetoptionen" des Internet Explorers wechseln Sie zunächst in den Tab für "Sicherheit / Security". Dort fügen Sie das Web Interface von Citrix zu der Liste der vertrauenswürdigen Seiten / Trusted Sites hinzu. Alternativ können Sie auch in der Registry den MIME-Filter deaktivieren. Dazu geben Sie dem folgenden Schlüssel einfach einen beliebigen anderen Namen: "HKEY_CLASSES_ROOT \ PROTOCOLS \ Filter \ application / x-ica 3". Nach diesen Schritten loggen Sie sich zunächst aus dem Web Interface aus und starten abschließend den Browser neu. Die Anwendungen sollten sich nun wieder wie gewohnt öffnen lassen. *(Citrix / ln)*

Der SharePoint Explorer bietet neben zahlreichen Erleichterungen bei der Arbeit in SharePoint mit "My Outlook" eine elegante Verbindung zum Mail-Client

Tools

Für Nutzer wie auch Administratoren kann die Arbeit in komplexen **SharePoint**-Farmen leicht unübersichtlich werden. Für den Anwender stellt sich oft die Frage, in welcher Site bestimmte Inhalte zu finden sind. Und ungeübte Nutzer verlieren sich gern im Dschungel der zahlreichen Sites im SharePoint-Intranet. Aber auch für den IT-Verantwortlichen ist es enorm wichtig, schnell in SharePoint navigieren zu können.

Für Microsofts Internet Explorer stellt daher die Dot Net Factory ein Add-In namens **SharePoint Explorer 2.0** kostenlos bereit, das sowohl die Navigation als auch die Arbeit mit SharePoint vereinfachen soll. Dazu liefert der SharePoint Explorer Anwendern und Administratoren eine **Baum-Ansicht der SharePoint-Struktur**, die alle Sites sowie den gesamten Inhalt übersichtlich darstellt. Diese Baum-Struktur visualisiert alle SharePoint Areas, Sites, Dokumentenbibliotheken und -Listen in jedem gewünschten Detailgrad. Dies ermöglicht dem Nutzer mit nur einem Klick an jeden Ort der SharePoint-Infrastruktur zu navigieren. Gleichzeitig bietet der SharePoint Explorer eine schnelle Suche in jeder Site. Inhalte lassen sich durch die Einbindung von SharePoint-Funktionalitäten in kontextsensitive Menüs, die durch einen einfachen Rechtsklick zu erreichen sind, schneller bearbeiten. Darüber hinaus ermöglicht das Tool über "My Outlook" den raschen Zugriff auf Microsofts Mail-Client. Zudem ist der Anwender in der Lage, Account-Daten so zu hinterlegen, dass er mühelos unterschiedliche Inhalte mit unterschiedlichen Accounts ansteuern kann. Zur Installation ist lediglich IE 6 oder höher sowie mindestens das .NET Framework 2.0 erforderlich. So bietet das Tool Zugriff auf die Versionen 2003 und 2007 von SharePoint (SharePoint 2010 nach Herstellerangaben in Vorbereitung) und unterstützt dabei jede beliebige Anzahl an SharePoint-Servern und -Sites. Als Bonbon bietet der Hersteller für diese kostenlose Software ein ausführliches PDF zu Installation und Konfiguration. Für den Download ist eine kurze Registrierung notwendig. *(jp)*

Link-Code: BBPE1

Bei der Softwareverteilung mit **Microsoft System Center Configuration Manager 2007** treffen Anwender oft auf ein ärgerliches und undurchschaubares Verhalten des SCCM: Dieser verlangt im Rahmen einer Installation eine Interaktion vom Anwender, quittiert diese dann aber mit einem Fehler. Ein typisches Szenario, in dem es zu diesem Problem kommt, ist das Rollout neuer Hardware an eine große Anzahl von Anwendern. Typischerweise sind die wichtigsten Applikationen von der IT vorinstalliert und die Bespielung mit seiner Abteilungs- oder Spezialsoftware über SCCM 2007 muss der Nutzer nach dem ersten Boot selber anstoßen. Doch oft erhält er dann die Fehlermeldung, dass bereits eine Installation im Gange sei. Dieser recht verbreitete Fehler besagt im Grunde nichts weiter, als dass der SCCM-Client bereits mit einer anderen Installation beschäftigt ist. Doch leider steht dem User keinerlei Information über den Status des Clients zur Verfügung, so dass er nie wissen kann, wann Zeit für die gewünschte Installation ist.

Hier hilft ein kleines, kostenloses Gadget weiter, das unter dem Namen **System Center Configuration Manager Status Indicator (CSI)** dem Anwender mit einem Ampel-System signalisiert, wann die rechte Zeit für eine Installation ist. Denn dieses Verhalten des

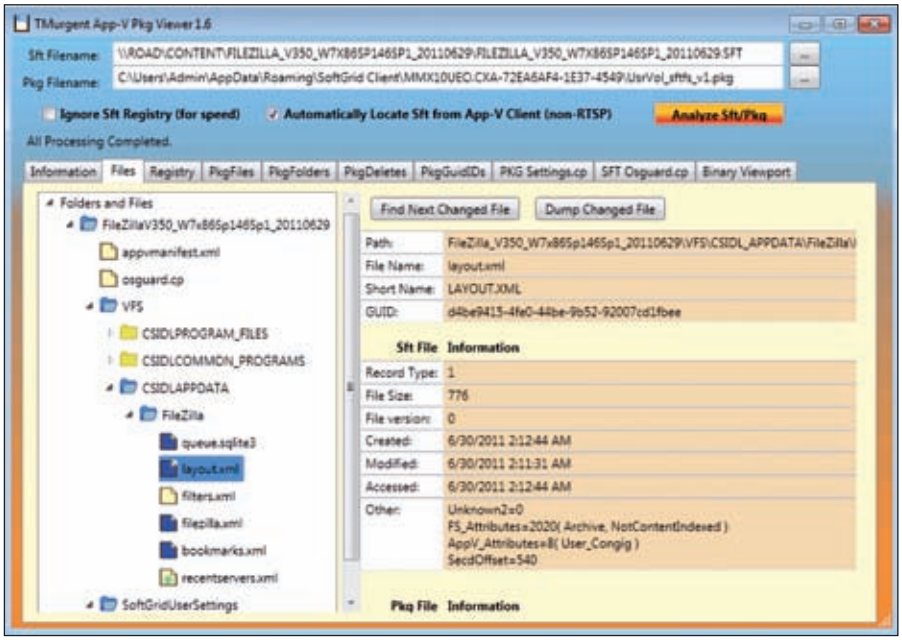
SCCM ist seitens Microsoft gewollt und lässt sich nicht ohne weiteres beeinflussen und auch die Bordmittel, die **den aktuellen Installations-Status visualisieren**, sind nicht sehr Anwenderfreundlich. CSI hingegen informiert den Nutzer übersichtlich und durch seine Gadget-Natur schnell erreichbar über den aktuellen Status von Installationen wie auch Deinstallationen auf seinem Rechner. Auch erhält der Anwender Hinweise zu notwendigen Reboots oder Logoffs. CSI steht in drei Varianten zur Verfügung: Das "CSI User Gadget" ist eine einfache Anwendung, die in den Ampelfarben den aktuellen Status des SCCM-Clients anzeigt. Das "CSI Power User Gadget" bietet zusätzlich erweiterte Informationen, wie etwa eine chronologische Auflistung aller getätigten Installationen. Und der "CSI Client" steht schließlich für Betriebssysteme zur Verfügung, die keine Windows-Gadgets unterstützen. Alle drei Varianten stehen nach kurzer Registrierung kostenlos zum Download zur Verfügung. *(jp)*

*Link-Code:*BBPE2

Unter Microsofts Werkzeug zur Applikationsvirtualisierung **App-V** hat der Administrator **kaum eine Möglichkeit, Einsicht in die PKG-Dateien** zu nehmen, in denen die individuellen Anpassungen der Nutzer der jeweiligen Applikation gespeichert werden. Dies ist insofern ärgerlich, als dass der IT-Verantwortliche bei Problemen mit der Applikation keine andere Wahl hat, als das App-V-Paket für diese Anwendung für den User zurückzusetzen. Dies ist für den Anwender unschön, weil er somit alle seine persönlichen Einstellungen verliert.

Das freie Tool **PKG View 1.6** ändert diese missliche Lage, indem es den Inhalt der PKG-Dateien für den Admin zur Ansicht freigibt. Somit ist der Systembetreuer in der Lage zu identifizieren, welche **Änderungen am Dateisystem und an der Registry für ein bestimmtes App-V-Paket** eines Anwenders vorliegen und kann so unter Umständen den Fehler beheben, ohne das Paket zurückzusetzen. Dabei erlaubt das Werkzeug jedoch nicht das Bearbeiten der PKG-Datei. Vielmehr hat der Admin mit PKG View die Möglichkeit, getätigte Änderungen zu identifizieren und diese über die Kommandozeile im Kontext der Anwender-PKG zu ändern. *(jp)*

*Link-Code:*BBPE3



PKG View gibt dem Administrator Einblicke in die individuellen Anpassungen einer mit App-V bereitgestellten Applikation

In einer **Terminal Server oder auch Citrix XenApp-Umgebung** kann es zu einem unbemerkten Ressourcenverbrauch auf dem Server kommen, wenn der Anwender zwar seine zuvor genutzte Anwendung schließt, jedoch nicht die Verbindung unterbricht. Denn der Nutzer beendet gewöhnlich die Applikation, indem er das entsprechende Fenster schließt. Solange er aber die Verbindung zum Server nicht abreißen lässt, können noch Hintergrundprozesse der eben geschlossenen Applikation aktiv sein und so **unbemerkt Server-Ressourcen verbrauchen**. Es ist nicht schwer sich vorzustellen, dass dieses Phänomen bei hunderten Usern dem zentralen Server einiges an ungeplanten Kapazitäten abverlangt. Ähnliches gilt im Übrigen beim Einsatz von virtualisierten Anwendungen unter App-V.

Abhilfe schafft hier ein kostenloses Werkzeug namens **LaunchIT**, das dem Admin die Kontrolle über Child-Anwendungen und Prozesse zurückgibt. Gerade aktualisiert auf Version 5.0.1, erkennt das Tool die Beendigung eines Programms und identifiziert selbstständig alle zu beendenden Prozesse, so dass dem unnötigen Ressourcen-Verbrauch ein Riegel vorgeschoben wird. Dieses Verhalten steuert der Admin über die Kommandozeile. Neben dieser grundlegenden Funktionalität bietet die aktuelle Version eine Reihe von neuen Features:

- LaunchIT identifiziert und beendet nicht nur direkte Child-Prozesse, sondern auch indirekte. Dies schafft die interne Funktionalität von App-V nicht.
- Ein Prozess kann automatisch beendet werden oder aber der Anwender wird vorher über eine Dialogbox dazu befragt.
- Es lässt sich eine Liste keinesfalls zu beendender Prozesse hinterlegen.
- Prozesse lassen sich vor dem Anwender verstecken, werden aber dennoch mit der jeweiligen Anwendung beendet.

LaunchIT 5.0.1 ist mit 38 KByte ein sehr schlankes Tool, das ohne Installation läuft. *(jp)*

*Link-Code:*BBPE4

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

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

Download der Woche


Quelle: Jouke Van Keulen – 123RF

Datensicherheit bei NAS-Geräten

Gut behütet im RAID-Würfel

von Peter Böhret

Zentrale Datenhaltung ist auch für kleinere Unternehmen oder einzelne Filialen attraktiv, vor allem seit kostengünstige NAS-Lösungen diese Möglichkeit für schmalere Budgets zugänglich machen. Aber selbst wenn die meisten Netzwerkspeicher mittels RAID für Datenredundanz sorgen – ausschließen lassen sich Datenverluste nicht. Die richtigen Maßnahmen und Schritte bei der Einrichtung einer NAS-Lösung können jedoch das Risiko erheblich senken. Dieser Beitrag zeigt, was Sie bei Anschaffung und Betrieb eines NAS beachten sollten und warum ein RAID-System keinesfalls das Backup ersetzt.

Was NAS-Systeme für kleine und mittlere Unternehmen so interessant macht, ist ihr gutes Preis-Leistungsverhältnis, sie lassen sich einfach einrichten und auch mit einer kleinen IT-Mannschaft betreiben. Zum anderen gilt NAS als schnell und sicher: Es bietet gute Geschwindigkeiten für den Dateizugriff und lässt sich in der Regel als RAID konfigurieren, was den Schutz vor Datenverlust erhöht. Viele Unternehmen wiegen sich jedoch gerade wegen des RAID-Verbunds in trügerischer Sicherheit. Ein RAID erhöht zwar die Ausfallsicherheit, ist aber nicht mit einem regulären Backup gleichzusetzen, bei dem alle Daten auf ein anderes Speichermedium, möglichst an einem anderen Ort, gesichert werden.

Menschliche Fehler und Hardware-Ausfälle

Die Besonderheiten des NAS-Systems machen es einerseits zu einer relativ sicheren Lösung, die im Allgemeinen eine höhere Verfügbarkeit aufweisen kann als dedizierte Dateiserver. Andererseits erschweren sie aber die Wiederherstellung von Daten, falls es doch zu einem Ausfall oder Datenverlust kommt. Unternehmen sollten deshalb aufmerksam bleiben und sich nicht zu einem falschen Sicherheitsgefühl verleiten lassen. Denn auch komplexe, redundant ausgelegte Systeme können versagen, schon allein weil mit der Komplexität des Systems die Zahl der möglichen Fehler steigt.

Häufige Gründe für einen Datenverlust in NAS-Systemen sind Hardware-Fehler, wie zum Beispiel ein Lesekopf- oder Plattencrash oder ein Controller-Fehler. Auch ein Stromausfall kann zu einem Verlust von Daten führen. Daneben sind menschliche Fehler bei der Bedienung ein nicht zu vernachlässigender Faktor: Unerfahrene oder unaufmerksame Mitarbeiter löschen versehentlich Daten oder formatieren die Festplatte, lassen sie bei Wartungsarbeiten fallen oder sind unachtsam bei der Konfiguration. Ebenso sind auf der Software-Seite Fehler möglich: So können Daten beispielsweise verloren gehen, weil Sicherungsprozesse fehlgeschlagen sind oder weil Diagnose- oder Reparatur-Tools unsachgemäß eingesetzt wurden und Daten beschädigen. Computerviren und höhere Gewalt wie Feuer oder Hochwasser machen insgesamt nur einen relativ kleinen Anteil der Fälle von Datenverlust aus, führen aber oft zu vergleichsweise gravierenden Schäden.

Ein Unternehmen kann der Ausfall und Verlust von Daten bei einem NAS sehr empfindlich treffen. Denn schließlich liegen hier alle wichtigen Daten an zentraler Stelle vor, der Schaden kann also möglicherweise größer sein als beim Ausfall eines dedizierten Dateiservers. Ein Backup zusätzlich zur RAID-Konfiguration ist deshalb zwingend notwendig. Allerdings kann es bei großen Datenmengen durchaus vorkommen, dass das Zeitintervall für das Backup oder auch die Bandbreite des Netzwerks nicht ausreicht, um alle Daten zu sichern. Dann liegen eventuell genau die betroffenen Informationen nicht als Backup vor.

Eine Datenrettung auf NAS-Systemen ist zwar möglich, aber im Vergleich zu einfachen Festplatten-Systemen schon wegen der RAID-Konfiguration relativ aufwändig. Zudem arbeiten die meisten NAS-Systeme mit Netzwerkprotokollen wie NFS oder CIFS statt mit Standardprotokollen. Dies erschwert die Datenrettung zusätzlich. Gerade proprietäre Dateisysteme können die

Datenrettung verkomplizieren und machen eventuell ein umfangreiches Reverse Engineering notwendig, bevor Datenrettungs-Tools die Strukturen auslesen können.

In drei Schritten zum sicheren NAS

Die folgenden drei Schritte helfen Ihnen, ein NAS-System so sicher aufzusetzen, dass das Risiko für den Verlust von Daten minimal gehalten wird – und für den Fall der Fälle vorbereitet zu sein, damit Daten schnellstmöglich wieder zugänglich sind.

Schritt 1: Das richtige System wählen

Vor Anschaffung und Implementierung eines NAS-Systems sollten sich Unternehmen intensiv Gedanken darüber machen, welche Anforderungen sie an das System haben – und hierbei nicht nur Performance und Kapazitäten in Betracht ziehen, sondern besonders Sicherheitsaspekte berücksichtigen. Insgesamt sollte bei der Einrichtung eines NAS nicht überflüssig gespart werden. Wer Zusatzkosten für hochwertige Festplatten oder zusätzliche Hardware für die Einrichtung eines RAID 5 scheut, tappt schnell in die Schnäppchenfalle. Wer nicht in Kauf nehmen will, dass eventuell wertvolle Daten verloren gehen, sollte bei der Investition in Festplatten für das NAS auf sehr gute Qualität achten. Disks mit einer Zulassung für den Betrieb rund um die Uhr, schnellen Zugriffszeiten und großem Cache sind optimal. Am besten ist es außerdem, Festplatten aus unterschiedlichen Produktions-Chargen anzuschaffen. Denn Hardware aus einer Baureihe ist oft anfällig für die gleichen Fehler – sei es wegen Mängeln, die in der Produktion entstanden sind, sei es wegen des parallelen Lebenszyklus. Eine Auswahl von Festplatten verschiedener Chargen senkt das Risiko, dass die Disks innerhalb kurzer Zeit in einer Art Kettenreaktion ausfallen.

Ein weiteres Kriterium für die Auswahl des NAS ist das verwendete Dateisystem. Empfehlenswert sind Geräte, die etablierte Branchenstandards verwenden und beispielsweise mit einem Microsoft-Dateisystem oder Linux EXT3 und Linux EXT4 beziehungsweise XFS arbeiten. Wer Alternativen einsetzt, wie zum Beispiel proprietäre Formate mit wenig bis gar nicht dokumentiertem Dateisystem, bekommt im Fall eines Datenverlustes eventuell Schwierigkeiten. Denn für diese proprietären Systeme sind auch die Datenrettungsprozesse noch nicht etabliert, was eine Wiederherstellung verlorener Daten aufwändiger, langsamer und teurer macht.

Bei der Wahl des NAS-Systems kommen Einsteigerlösungen mit nur einer Festplatte für Unternehmen aus Sicherheitsgründen nicht in Frage. Egal wie groß oder klein das Unternehmen ist, ein RAID 5 ist als Minimum immer Pflicht. Die zusätzlichen Hardwarekosten müssen bei der Budgetplanung möglichst frühzeitig berücksichtigt werden, genauso wie Virenscanner, Firewall und eventuelle andere Sicherheitslösungen.

Schritt 2: NAS-Fahrplan aufstellen

Ist die Wahl für die Hardware und eventuell ergänzende Software gefallen, geht es an die Einrichtung und Inbetriebnahme des NAS. Da dies im Vergleich zu anderen Systemen relativ einfach ist, verfallen gerade kleine und mittlere Unternehmen oft dem Irrtum, dass jeder IT-Administrator ein NAS sicher einrichten kann. Allerdings kann es bei unsachgemäßer Behandlung zu einem Komplettausfall kommen, der eventuell einen größeren Datenverlust verursacht. Noch größer als bei der Ersteinrichtung ist diese Gefahr allerdings bei Erweiterungen bestehender NAS-Lösungen. Denn hier muss darauf geachtet werden, wie das bestehende System konfiguriert ist, außerdem sind bereits Daten auf dem System abgelegt, die im Zuge der Erweiterung nicht versehentlich gelöscht oder beschädigt werden dürfen.

Vor der endgültigen Inbetriebnahme sollten deshalb NAS-Lösungen und vor allem Erweiterungen von erfahrenem IT-Personal getestet werden. Wichtig ist außerdem eine sorgfältige Dokumentation des eingesetzten Systems und eventueller Zusatz- oder Erweiterungslösungen. Auch für die Einhaltung der Compliance und bei eventuellen Mitarbeiterwechseln in der IT-Abteilung spielt eine gründliche Dokumentation eine entscheidende Rolle.

Schritt 3: Backup mit Netz und doppeltem Boden

Wenn NAS-Lösungen als RAID konfiguriert werden, sind sie im Allgemeinen sehr sicher und gegen Ausfälle der Hardware gut geschützt. Wie so oft steckt jedoch der Teufel im Detail und Fälle, bei denen mehrere Festplatten gleichzeitig ausfallen, durch Bedienfehler Daten gelöscht oder beschädigt werden oder ein Feuer gleich mehrere Festplatten zerstört, sind durch die Einrichtung eines RAID nicht auszuschließen. Unternehmen sollten nicht davon ausgehen, dass ein RAID als Datensicherung ausreicht und ein regelmäßiges Backup ersetzen kann. Geschäftskritische Daten sollten regelmäßig auf anderen Speichermedien gesichert werden, damit sie sich bei einem Ausfall wiederherstellen lassen. Dies empfiehlt sich nicht nur für die seltenen Fälle, in denen eine Datenrettung auf dem NAS nicht mehr möglich ist. Denn gerade bei RAID-Systemen ist die Wiederherstellung von Daten relativ aufwändig. Ein regelmäßiges Backup beugt dem vor.

Der Prävention dient auch die frühzeitige Kontaktaufnahme mit einem Anbieter für Datenrettung. Zur Vorbereitung auf den Worst Case kann das Unternehmen mit einem solchen Experten planen, welche Rettungsmaßnahmen für welchen Fall angebracht sind und was im Fall eines Datenverlusts zu tun ist. Ein solcher Plan sollte integraler Bestandteil des Disaster Recovery sein. Das erspart viele Fehler, die sonst nach einem Datenverlust in der ersten Panik begangen werden. Rettungsversuche durch unerfahrenes Personal vergrößern den Schaden bei einem Datenverlust häufig noch und lassen die Daten eventuell ganz verloren gehen.

Ein Datenverlust lässt sich niemals ganz ausschließen und kann große Folgeschäden nach sich ziehen, wenn wichtige Unternehmensdaten nicht mehr verfügbar sind. Dieses Risiko lässt sich vermindern, wenn eine Versicherung gegen Datenverlust abgeschlossen wird. Sowohl für die Rettung von Daten nach Systemausfällen als auch für Datenverlust infolge von Feuer oder Wasser, Vandalismus, Einbruch, Kurzschluss sowie Über- und Unterspannung gibt es Versicherungen. Diese decken dann weit mehr ab als die üblichen Versicherungen gegen Hardware-Ausfälle, die nur die Hardware-Kosten berücksichtigen – häufig weit weniger als der Wert der gespeicherten Informationen. *(ln)*

Peter Böhret ist Managing Director bei Kroll Ontrack.

Malware-Schutz beim Landessportbund Nordrhein-Westfalen

Sicherheit im Handumdrehen

von Klaus Jetter

Ein oft unterschätztes Einfallstor für Malware sind mobile Devices wie Smartphones und Notebooks, die von Außendienstmitarbeitern genutzt werden. Daneben besitzen kleine und mittlere Unternehmen oftmals nur eingeschränkte Ressourcen und Budgets für ihre IT-Sicherheit. Das bedeutet, dass die Sicherheitssoftware nicht immer auf dem neuesten Stand ist, da Wartungsaufgaben oftmals noch manuell durch den Administrator durchgeführt werden müssen. Einem ähnlichen Szenario sah sich bis Ende letzten Jahres auch die IT-Abteilung des Landessportbunds Nordrhein-Westfalen ausgesetzt. Mit der F-Secure Business Suite sollte sich das ändern.

Der Landessportbund Nordrhein-Westfalen setzt auf F-Secure zur Absicherung seiner Rechner

Es war unter anderem das Update-Verhalten der bestehenden Antiviren-Software, verbunden mit einem hohen personellen Aufwand, das den Landessportbund Nordrhein-Westfalen nicht zufrieden stellte. Aufgrund der mangelnden Unterstützung der immer häufiger eingesetzten 64 Bit-Versionen von Windows XP und Windows 7 auf den Arbeitsplatzrechnern wurden immer mehr lokale und ungemanagte Einzelplatzversionen verschiedenster Hersteller installiert, um die bestehenden Lücken zu schließen. Eine zentrale Verwaltung der Sicherheitsinfrastruktur war aufgrund dessen kaum mehr möglich und die Situation mit den verteilten Systemen insgesamt nicht mehr tragbar. Erschwerend kam hinzu, dass der Landessportbund viele Außendienstmitarbeiter hat, die mit mobilen Geräten ausgerüstet sind. Deren Einbindung in das Kernnetz verursachte zusätzliche Herausforderungen. Insgesamt erforderte die Administration oftmals mehrere Arbeitsstunden pro Woche – insbesondere dann, wenn die Virendatenbanken auf den neuesten Stand gebracht werden mussten oder ein Virenscan nötig war. Updateverlauf und der Status des Scans mussten jeweils pro System überwacht werden.

Erfüllbare Wünsche

Die IT-Verantwortlichen rund um Georg Hopp, Referatsleiter IT des Landessportbunds NRW e.V., stellten daraufhin einen Forderungskatalog an die zukünftige Sicherheitslösung zusammen, der Folgendes beinhaltete: Während des Roll-Outs sollte die neue Security Suite bereits installierte AV-Scanner automatisch erkennen und eine selbständige Deinstallation dieser Programme vornehmen. Die Erstellung von Sicherheitsrichtlinien für Clients und Server sollte ebenso einfach vonstattengehen wie das Einbeziehen von weiteren Rechnern und Lizenzen in das existierende Security-Netz. Ebenso wichtig war die Möglichkeit der Einbindung von mobilen Geräten in die Sicherheitsinfrastruktur inklusive automatischem Update der darauf installierten AV-Software – sowohl bei einer Verbindung mit dem Kernnetz des Landessportbundes als auch bei unabhängiger Nutzung des Internets. Letztlich wurde darüber hinaus auf ein intuitives und zentrales Management der Sicherheitslösung Wert gelegt.

Der Landessportbund entschied sich nach der Ausschreibungsphase aufgrund der umfassenden und kompetenten Beratung für den zertifizierten F-Secure Gold-Partner R. Bücker EDV-Beratung Datentech-

nik GmbH aus dem ostwestfälischen Hille. Aufgrund des Forderungsprofils empfahlen die Berater die F-Secure Business Suite, da damit eine Einbindung mobiler Nutzer sowie ein aktueller Überblick über die Infrastruktur und eine Automatisierung des Updates aller Virendatenbanken möglich ist. Für die mobilen Geräte soll dann später der F-Secure PSB (Protection Service for Business) als gemanagte Lösung eingesetzt werden. Georg Hopp begründet die Entscheidung wie folgt: "Ein schlankes und intuitives Management sowie eine gemanagte Anti-Virus-Lösung konnte uns nur F-Secure bieten. Die Flexibilität und der Überblick über unseren Virenschutz sind damit enorm gestiegen."

Roll-out in einem Tag

Für die Installation vor Ort waren zwei Tage veranschlagt, in denen die Grundinstallation der Business Suite inklusive der dazugehörigen Konfiguration und Erstellung der Richtlinie für Clients und Server vorgenommen wurde. Durch die einfache Struktur des Managements konnte dies aber bereits während der ersten Hälfte des ersten Tages gelöst werden. Dabei wurde die Client Security-Software als Paket in den Policy Manager eingelesen und in kleinen Gruppen parallel auf die Clients verteilt. Aufgrund der Übersichtlichkeit und der Möglichkeit, eine zentrale Konfiguration vorzugeben, traten laut Georg Hopp keinerlei Schwierigkeiten während des Implementationsprozesses auf. Deshalb konnte die zweite Hälfte des Tages für einen Testrollout auf zwei Servern und fünf Workstations genutzt werden, wobei das Verhalten der Maschinen bei der Umstellung kontrolliert und das Neustartverhalten geprüft wurde. Auch hier konnten die Benutzer auf ihren Arbeitsplatzrechnern weiterarbeiten, ohne dass es zu Beeinträchtigungen oder sonstigen Störungen kam.

Während des zweiten Tags wurde ein Stand-Alone-Paket mit der Client-Security-Lösung konfiguriert und getestet, um deren Schutzwirkung in Hinblick auf durch das Kernnetz unverwaltete Systeme überprüfen zu können. Dieses Paket stand anschließend den Außendienstmitarbeitern auf CD oder USB-Stick zur Verfügung. Es enthält sämtliche Konfigurationen sowie eine Lizenz und kann per Doppelklick ohne weitere Userabfragen installiert werden. Ebenso ist es fähig, inkompatible Drittanbieter-Software automatisch zu deinstallieren, falls das notwendig sein sollte. Im Lauf des Tages konnte dann im restlichen Netzwerk der Roll-out in Gruppen fortgesetzt werden, sodass abends insgesamt 120 Systeme (17 Server, 103 Clients) umgestellt waren. Die restlichen Systeme setzte die IT-Abteilung des Landessportbundes NRW in Eigenregie auf.

IT-Sicherheit auf Autopilot

Für Georg Hopp ist ein erfolgreiches Sicherheitsmanagement von Unternehmensrechnern und -Servern von drei Faktoren abhängig: der Stabilität, der Geschwindigkeit und der Effizienz einzelner Abläufe. Eine Reduzierung des Arbeitsaufwandes durch Automatisierung setzt für den IT-Leiter Ressourcen frei, die es ihm und seinem Team ermöglichen, sich auf die Lösung anderer IT-Probleme zu konzentrieren. Hier spielt ihm der Policy Manager der Business Suite in die Hände. Dieser verwaltet täglich anfallende Arbeiten wie den Schutz neuer Computer, den Import und das Entfernen neuer oder getrennter Hosts und ermöglicht aufgrund der Active Directory-Integration die sofortige Replizierung der Microsoft Active Directory-Struktur – Abläufe, die den IT-Administrator des Landessportbundbunds mehrere Stunden oder sogar einen ganzen Arbeitstag pro Monat gekostet haben. Das zentralisierte Sicherheitsverwaltungssystem erspart außerdem den Weg in jedes einzelne Büro, um die Updates aufzuspielen; Sicherheits-Policies können augenblicklich geändert und im gesamten Netz verteilt werden.

Daneben bietet die Business Suite Schutz für Workstations und Laptops (Client Security, Anti-Virus for Workstations), Server (Anti-Virus for Windows Servers, Anti-Virus for Citrix Servers) und Schutz für E-Mail sowie einen Webfilter (Internet Gatekeeper for Linux, Anti-Virus for Microsoft Exchange mit Spam Control). Zu den erweiterten Funktionen gehören ein reputationsbasierter Exploit Shield und die Browsing Protection als Schutz gegen Spam sowie eine Rootkit-Erkennung gegen verborgene Malware und Intrusion Prevention. Das Sicherheitspaket bietet somit automatisierten Echtzeitschutz vor Viren, Würmern, Spyware und Trojanern unter anderem auch auf Grundlage von Cloud Computing-Technologie.

Geplant: Schutz für mobile Mitarbeiter

Für das Schulnetz des Landessportbundes wurden inzwischen weitere Lizenzen nachbestellt, die über das bestehende Management eingebunden und ohne weitere Hilfe in Betrieb genommen werden konnten. In der nächsten Stufe sollen die mobilen Benutzer mit der F-Secure PSB-Lösung (Protection Service for Business) ausgestattet werden. Dabei handelt es sich um eine Cloud-Lösung, bei der die Clients über die F-Secure Security Server verwaltet und aktualisiert werden. Viele der mobilen Systeme sind nur sehr selten im Netzwerk des Landessportbundes, sodass nur über diese gemanagte Lösung die dauerhafte Aktualität der Virendatenbanken und das Wissen darüber gesichert sind. Das Produkt verfügt bereits im Auslieferungszustand über sieben vordefinierte Sicherheitsprofile für verschiedene Endkundenanwendungen.

Fazit

Im Netzwerk des Landessportbunds NRW e.V. werden nun die Sicherheitslösungen von F-Secure zur internen Verwaltung und zum Virenscan innerhalb des Netzes verwendet. Aufgrund der vereinheitlichten Infrastruktur ist die Administration wesentlich übersichtlicher und vereinfacht worden. Infolge dessen hat sich auch der Personalaufwand reduziert. Ferner ist das Updateverhalten zuverlässiger und regelmäßiger im Gegensatz zu früher geworden. Georg Hopp ist sehr zufrieden mit der neuen Sicherheitslösung: "Noch nie habe ich ein Rollout einer Software erlebt, das so problemlos gelaufen ist. Außerdem haben wir eine enorme Zeiteinsparung bei der Administration. Als nächsten Arbeitsschritt möchten wir die Installation der F-Secure Software auf unseren mobilen Geräten angehen." *(dr)*

Klaus Jetter ist Country Manager bei der F-Secure GmbH.

Berechtigungsmanagement bei der Sovello AG

Rechtevergabe wie am Fließband

von Oliver Fischer

Im Zentrum der öffentlichen Diskussion um Industriespionage, Produkt-Piraterie und Datenlecks in Unternehmen steht die grundlegende Frage: Wer darf was wann lesen? Mit dieser Problematik sah sich auch der Hersteller von Solarmodulen, die Sovello AG aus Bitterfeld-Wolfen, konfrontiert. Um sensible Daten zu schützen und den produktiven Betrieb trotzdem nicht unnötig zu behindern, war eine smarte Lösung für die Vergabe von Zugriffsberechtigungen für Personen und Personengruppen gefragt. Unsere Reportage zeigt, welche Funktionen das Werkzeug zum Rechtemanagement mitbringen musste und ob es diese Anforderungen erfüllt hat.

Die Sovello AG produziert Solarwafer, Solarzellen und Solarmodule. Das Unternehmen betreibt drei Produktionsstätten in Bitterfeld-Wolfen in Sachsen-Anhalt und beschäftigt dort rund 1.250 Mitarbeiter. Mit der kürzlich erfolgten Fertigstellung der dritten Anlage hat die nominale Produktionskapazität des Unternehmens etwa 180 Megawattpeak erreicht. Mehr als die Hälfte der Beschäftigten sind IT-Anwender – sämtliche Bereiche und Geschäftsprozesse basieren auf IT-Leistungen. Im Rahmen eines Projektes zur Verbesserung der Transparenz von IT-Leistungen entschied sich das Unternehmen Anfang 2010 dafür, auch das Berechtigungsmanagement in einer von zwei Domänen mit zirka 500 Anwendern und Datenbeständen auf zwei Fileservern zu optimieren.

Das Ziel: mehr Übersichtlichkeit

Die IT-Verantwortlichen des Solar-Fabrikanten suchten nach einer Lösung, die nicht nur in der Lage sein sollte, die vergebenen Berechtigungen für das IT-Management und die Geschäftsführungsebene übersichtlich zu visualisieren, um potenzielle Sicherheitslücken frühzeitig zu erkennen. Parallel dazu galt es, den eigentlichen Datenproduzenten und -inhabern mehr aktive Verantwortung für ihre Daten zu übertragen. Damit, so die Zielsetzung, sollte es zum einen zu einer Entlastung der IT-Abteilung kommen. Außerdem setzte die Sovello AG darauf, dass sich der Schutz sensitiver Daten immer dann verbessert, wenn es möglich ist, Berechtigungen für Dateizugriffe mit dem Wissen um Inhalte und Wertigkeit der Dokumente zu vergeben.

Eine Lösung dieser Aufgabe zeichnete sich ab, als Onnen Schenk, der IT-Leiter von Sovello, im Rahmen einer Informationsveranstaltung im Januar 2010 die Berechtigungsmanagementlösung 8MAN des Software-Herstellers protected-networks.com kennenlernte. Die Software für das Berechtigungsmanagement in Server-Umgebungen analysiert selbständig alle vergebenen Zugriffsrechte innerhalb der Windows-Server-Umgebung. Bei der Vergabe von Berechtigungen orientiert sich das Werkzeug an den etablierten Arbeitsabläufen in Unternehmen. So lässt sich bei der Erstellung der Gruppen die interne Organisation des Unternehmens als Grundlage heranziehen und abbilden, gegliedert etwa nach Standorten, Abteilungen oder Kostenstellen. Domänen, Freigaben und Verzeichnisse lassen sich optional den Dateninhabern, Fachabteilungen oder auch dem Helpdesk zuweisen. Änderungen kann so direkt der Dateneigentümer durchführen – die Einhaltung übergreifender Vorgaben der IT-Administration ist dabei durch frei definierbare Regeln gewährleistet, die sich automatisiert durchsetzen lassen.

Mit dieser an den realen Arbeitsabläufen in Unternehmen ausgerichteten Funktionalität sah Schenk die grundlegenden Anforderungen von Sovello abgedeckt: “Aus meiner Sicht bot diese Software mindestens zwei für uns wichtige strategische Potentiale: Zum einen gewährleistet sie die Transparenz-Verbesserung der Berechtigungsstrukturen für Anwender und Management. Zum anderen erlaubt es 8MAN, ausgewählte Berechti-

gungsprozesse perspektivisch auch Nicht-Administratoren zu übertragen."

Testphase mit positiven Ergebnissen

Um zu verifizieren, inwieweit die theoretischen Vorzüge der Lösung im praktischen Betrieb greifen, unterzog Sovello die Lösung einer intensiven dreimonatigen Evaluierungsphase. "Wir konnten Funktionen innerhalb einer Testinstallation prüfen und standen in einem engen Dialog mit den Beratern und Technikern, so dass alle unsere Fragen ausführlich diskutiert und beantwortet werden konnten.

Als besondere Stärke des Herstellers sehen wir hier, dass man unseren Anregungen immer aufgeschlossen gegenüberstand und sich einige Ideen innerhalb kürzester Zeit bereits in der Lösung wiederfanden", führt Schenk aus. Zum Ende der Testphase war man bei Sovello davon überzeugt, mit 8MAN exakt das gefunden zu haben, was man suchte. So konstatiert Schenk: "Maßgeblich für unsere Entscheidung waren insbesondere sowohl der hohe Grad an Deckung mit den Vorgaben unseres Pflichtenhefts als auch das erkennbar große Potenzial für die Weiterentwicklung sowie das hohe Engagement bei der Betreuung durch den Hersteller und den Service-Partner."

Implementierung an einem Tag

Als Ergebnis aus den erfolgreichen Tests erfolgten im dritten Quartal 2010 die Auftragserteilung sowie die Installation. Mit der endgültigen Übernahme in den Produktivbetrieb wartete Sovello allerdings noch bis zum vierten Quartal 2010, da das Unternehmen dem Software-Hersteller etliche Wünsche für benötigte Reports mitgeteilt hatte und dieser zusagte, diese in einem Folge-Release von 8MAN umzusetzen. Dies stand dann mit dem gewünschten Funktionsumfang im November 2010 zur Verfügung, so dass das Programm ab diesem Zeitpunkt in den vollen Einsatz gehen konnte.

Insgesamt hielt sich der Aufwand für das Roll-out auf der vorhandenen Hardware in Grenzen. Da die Software ja bereits als Evaluation-Version auf dem System aufgespielt war, mussten lediglich eine Aktualisierung des Lizenzschlüssels sowie ein Update auf die aktuelle Version erfolgen. Probleme traten bei der Installation keine auf, da gründliche Vorarbeit geleistet und alle Anforderungen und Voraussetzungen im Vorfeld abgestimmt worden waren.

Anschließend erfolgte live am Produktivsystem eine Besprechung der Neuerungen, bei der sich noch anstehende Fragen klären ließen. Der Zeitaufwand für die gesamte Installation der Software auf der vorhandenen Hardware einschließlich der Schulungsmaßnahmen für die Mitarbeiter in der IT-Administration war mit nur einem Tag relativ kurz.

Die kurzen Kommunikationswege zum Hersteller nutzt Sovello weiterhin, um Vorschläge für mögliche Funktionen in kommenden Software-Versionen zu unterbreiten. "Wir stehen mit protected-networks.com wegen einer noch einfacheren Gestaltung der Reports und in Bezug auf perspektivische Implementierung weiterer Hosts, wie beispielsweise Datenbank- und Mailserver, in Kontakt", so Schenk. Theoretischer Natur blieben bislang die Erfahrungen mit dem Support. "Das liegt allerdings nicht an dessen Erreichbarkeit, sondern ist dem Produkt geschuldet. Denn", so Schenk, "es sind bislang keinerlei Störungen aufgetreten und zur Bedienung gab es bislang bis auf die bei der Installation hinreichend geklärten Fragen keinen weiteren Auskunftsbedarf."

Fazit

Insgesamt nutzen derzeit die fünf Mitarbeiter der IT-Administration von Sovello 8MAN, um die Zugriffsberechtigungen auf dem Server des Unternehmens zu managen, wobei vor allem Recherchen im Vordergrund stehen. Es gilt, Nutzerrechte innerhalb der Anwenderschaft angesichts umfangreicher Berichte und Reports effektiver zuzuordnen und Gruppenzusammenhänge, die oftmals zu Überberechtigungen führen, aufzulösen. Schenk sieht sich in der Entscheidung bestätigt, denn die gestellten Anforderungen an die Funktionalität des Programms – Automatisierbarkeit, Schnittstelle zur Prozessintegration für den Versand von Berichten – sind durchweg erfüllt.

Auch das Benutzer-Frontend konnte laut Schenk überzeugen: "Übersichtlichkeit und Ergonomie sind für das Berechtigungsmanagement unverzichtbar, denn Werkzeuge, die bei Mitarbeitern keine Akzeptanz gewinnen, werden nicht konsequent eingesetzt. Hier konnte 8MAN ebenfalls punkten, denn im Bereich der IT-Administration sind wir von Anfang an ausgezeichnet zurechtgekommen. Nachholbedarf haben wir allenfalls intern, damit die Verantwortlichen als Report-Adressaten die Informationen aus den bereitgestellten Berichten für ihre Bereiche wirklich in vollem Umfang ausnutzen, um letztendlich mehr aktive Verantwortung für ihre Daten zu übernehmen." *(ln)*

Die Kluft zwischen Dateneignern und IT-Abteilung

Vornehmlich bildet das Berechtigungsmanagement einen wesentlichen Aspekt im Gesamtkontext des IT-Sicherheitskonzepts eines Unternehmens. Problematisch wird es allerdings oftmals, wenn es darum geht, die Verantwortlichkeit für die Daten und darüber die Zugriffsrechte für Personen oder Personengruppen zu definieren. Aus Sicht der IT-Abteilung, die über das technologische Know-how verfügt, sind schützenswerte Dateien lediglich eine in ihrer Größe klar definierte Menge an Byte. Ein Wissen um die Inhalte dieser Dateien, über ihre Sensibilität und über die Personen, denen aufgrund der in einer Datei enthaltenen Informationen der Zugriff gewährt beziehungsweise verweigert werden muss, ist aus technischer Sicht nicht notwendig und fehlt entsprechend meist. Das gilt insbesondere dann, wenn im Zuge der IT-Industrialisierung externe Serviceprovider die Berechtigungsstrukturen administrieren und organisieren.

Auf der anderen Seite sind die Anwender, die – meist als Dateneigner – die Schutzwürdigkeit der Informationen kennen, meist keine IT-Spezialisten. Häufig führt dies zu einer fehlenden Akzeptanz für die von IT-Abteilungen diktierten Lösungen zum Berechtigungsmanagement und zu einer mangelnden Sensibilisierung in puncto Sicherheitsfragen. Zudem stockt vielfach der Informationsfluss zwischen Fachabteilung und IT-Spezialisten.

Ein logischer Ausweg ist es daher, Datenerzeuger und -eigner in die Lage zu versetzen, das Berechtigungsmanagement selbst zu übernehmen. Dafür muss sich aber eine entsprechende Lösung nicht nur aus technologischer Sicht für den Einsatz qualifizieren, sondern auch aus Anwendersicht. Lapidar gesagt: Eine programmiertechnisch ausgefeilte Lösung nutzt wenig, wenn es ergonomisch klemmt. Denn die Folge sind falsch oder verspätet gesetzte Zugriffsberechtigungen, durch die die Datensicherheit nachhaltig gefährdet wird.

Als Opa Admin war: IBM AN/FSQ-7

Movie Star

von John Pardey

Kaum etwas dürfte unsere Vorstellung von Rechnern mehr geprägt haben als die Mainframes – raumfüllende Blechgiganten, die Daten mit sagenhafter Geschwindigkeit verarbeiten. Der IBM AN/FSQ-7 wird diesem Bild mehr als gerecht, belegte er doch vier komplette Stockwerke, wog 275 Tonnen und ist einer von Hollywoods beliebtesten Nebendarstellern.

Eigene Hausnummer

Der AN/FSQ-7 wurde in den 50er Jahren von der IBM für die US Air Force entwickelt, die insgesamt 52 dieser Mainframes im SAGE-Luftabwehrsystem vereinte. Jeder Einzelne dieser Rechner beanspruchte 2.000 Quadratmeter und da jeweils zwei Instanzen an einem Standort zwecks Ausfallsicherheit gleichzeitig betrieben wurden, füllte er ein komplettes vierstöckiges Haus. Somit ist er der größte jemals gebaute Computer und wird diesen Titel höchstwahrscheinlich auch nicht wieder abgeben müssen.

Da die Admins jedoch keine ausgebildeten Systemspezialisten, sondern einfache Soldaten waren, entwickelte die IBM erstmals einfach zu bedienende Schnittstellen. Dazu gehörte die für uns selbstverständliche Ausgabe von Bildern und Texten in Echtzeit auf einem Bildschirm ebenso wie die Bedienbarkeit mit einem "Lichtgriffel" – einem Vorläufer der Maus. Gleichzeitig eröffnete die notwendige Vernetzung aller AN/FSQ-7 im SAGE-System das Zeitalter der Modems und des WAN.

Projekt gescheitert

Doch der Nutzen der AN/FSQ-7-Mainframes im SAGE-System war für die Landesverteidigung schon mit der Inbetriebnahme nahe null, denn das System war darauf ausgelegt, klassische Luftangriffe zu orten. Doch mit dem ersten Booten waren Interkontinentalraketen die erste Wahl der Waffen und SAGE konnte diese nicht aufspüren. Dieser klassische Projektflop erwies sich dennoch für die IBM als Glücksfall. Denn mit der Entwicklung des AN/FSQ-7 hatte die Firma derart viel Know-how über Großrechensysteme aufgebaut, dass die bekannte, marktdominierende Stellung der Zukunft hier ihr Fundament fand. Gleichzeitig wurden dem AN/FSQ-7 zivile Aufgaben in der Luftsicherung zuteil – und Hollywood auf ihn aufmerksam.

Walk of Fame

Auch wenn Sie heute unter Umständen zum ersten Mal vom AN/FSQ-7 gehört haben, ist die Chance, dass Sie ihn schon einmal gesehen haben, ziemlich groß. Denn schon in den 60er Jahren begann Hollywood den Mainframe – komplett, oft aber auch in Teilen – als Requisit zu nutzen. So wirkte er bis heute in über 100 Produktionen mit. Etwa in den berühmten "Batman"- und "U.N.C.L.E."-Fernsehserien aus den 60ern und dem "Planet der Affen" von 1973. Fehlen durfte der AN/FSQ-7 natürlich auch nicht im Hacker-Klassiker "Wargames" von 1983. Und der Mainframe weist eine Karriere auf, die sich viele Hollywood-Größen wünschen, denn sein Erfolg setzte sich in den 90ern in "Independence Day" ebenso fort wie in unseren Tagen, etwa in der Fernsehserie "Lost". Ob es eines Tages noch für einen Oscar reicht, bleibt jedoch (leider) fraglich.

Als Rechner schnell sinnlos, dann aber bei Film und Fernsehen durchgestartet: der IBM AN/FSQ-7

Old School Backup & Recovery

Im Web finden sich Erfahrungsberichte von Admins früher Mainframes, die von kuriosen Backup & Recovery-Konzepten berichten. Dabei stellten die Operatoren vor ihrer Konsole eine Halterung auf, in der sich eine Polaroid-Sofortbildkamera befestigen ließ. Zeigte der Mainframe nun Anzeichen eines Systemversagens, machte der Admin in Windeseile ein Polaroid seiner Konsole. Nachdem er dann den Rechner neugestartet hatte, um die aufgetretenen Probleme zu beseitigen, brachte er seine Konsole mit Hilfe des eben gemachten Fotos wieder auf den Stand von vor dem Absturz. Gewusst wie!

Debian GNU/Linux, 4. aktualisierte Auflage

Debian hat in den vergangenen Jahren eine unglaubliche Akzeptanz erfahren. Der Hauptgrund: Zuverlässigkeit gepaart mit gesteigerter Benutzerfreundlichkeit. Die Verbreitung und das Verständnis im Umgang mit Debian weiter voranzutreiben, ist der Anspruch dieses Werkes, das Debian 6 "Squeeze" als Grundlage verwendet.

In drei Teile untergliedert, fächert sich der Inhalt ausgewogen zwischen Installationsbeschreibungen, Desktop-Einsatz und Administration auf. Im ersten Abschnitt vollzieht Autorin Heike Jurzik die Installation über verschiedene Medien nach, was bereits bei den Überlegungen zuvor beginnt. Detailreich wird die Paketverwaltung betrachtet, bevor die Komponenten Netzwerk und Internet sowie Drucken den nötigen Platz finden. Debian als Desktopsystem zu verwenden, wirkt für die Ohren manches Power-Users fremdartig. Doch das Betriebssystem ist modern und kann sich auch dieser Herausforderung stellen. Damit Konsoleros daran nicht scheitern, ist zirka ein Drittel des Buchumfangs in diesen Part investiert worden.

Erfreulich, dass die Autorin keine Vorgaben bezüglich des Window-Managers tätigt und sowohl GNOME, KDE SC 4 wie auch alternativen Umgebungen gleichermaßen Platz einräumt. Fortgeschrittene Anwender und Administratoren werden im dritten und umfangreichsten Teil fündig. Ausführliche Einblicke in den Linux-Background, wie Texteditoren, Zugriffsrechte, Dateisysteme, Benutzer- und Prozessverwaltung, Jobs oder die Shell, lassen keine Fragen offen. Für das Internet relevante Techniken oder Dienste wie DHCP, BIND, Mail, HTTP, FTP oder Sicherheitsaspekte werden ebenso dargestellt, wie auch Samba und GRUB nicht fehlen können. Den Abschluss bilden das Upgrade auf Squeeze sowie ein Mini-einblick in die Kernelkompilierung.

Fazit

Das Buch führt den Leser Stufe für Stufe nach oben auf dem Weg zum Debian-Experten. Die Autorin vollzieht ihre Erläuterungen dabei sehr ausführlich und didaktisch gut nachvollziehbar. Aufgrund des Umfangs entstand so nebenbei ein aktuelles Referenzwerk. Auf der beiliegenden DVD befindet sich Debian Squeeze. Nicht zuletzt bemerkenswert ist wohl auch der Fakt, dass eine weibliche Autorin das knapp 800-seitige Werk vorgelegt hat. *Frank Große*

Autor	Heike Jurzik
Verlag	Galileo Computing
Preis	39,90 Euro
ISBN	978-3-8362-1694-4
Bewertung *(max. 10 Punkte)*	**10**

Linux-Server einrichten und administrieren

Das Buch "Linux-Server einrichten und administrieren", das den Hinweis "Kein Vorwissen erforderlich" trägt, hat ambitionierte Linux-Neulinge im Visier. Der Inhalt gliedert sich in drei Teile: Installation, Handbuch und Workshops. Zu erwähnen ist, dass sich das Buch auf Debian Squeeze fokussiert und andere Distributionen nicht berücksichtigt.

Das Kapitel zur Installation des Debian-Servers ist mit 40 Seiten recht knapp bemessen und für den absoluten Neueinsteiger etwas zu sehr im Unix-typischen komprimierten Sprachstil geschrieben. Inhaltlich ist nichts zu beanstanden, aber der eine oder andere Neuling wird hier möglicherweise doch auf Sekundärliteratur oder das Internet zurückgreifen müssen. Die Kapitel des mit "Das Handbuch" betitelten zweiten Teils sind größtenteils in beliebiger Reihenfolge lesbar. So lernt der Leser neben einem Abriss zu Unix/Debian die Arbeitsweise der Shell und Konsole kennen.

In den Kapiteln zu Netzwerken versucht der Autor den Spagat zwischen theoretischem Hintergrundwissen und praktischer Anwendung zu finden – was ihm nicht immer gelingt. Für Einsteiger ist der theoretische Inhalt möglicherweise zu komprimiert, um sofort nachvollziehbar zu sein. Das Themenspektrum erstreckt sich über TCP/IP, DNS, DHCP, IPv6, das Sammeln von Informationen im Netzwerk sowie die grundlegenden TCP/IP-Dienste und Netzwerksicherheit. In den weiteren Kapiteln werden so ziemlich alle unter Linux verfügbaren Server vorgestellt und beschrieben: Dateiserver, Datenbankserver, Webserver, DNS- und Mailserver. Das X-Windows-System und virtuelle Maschinen tauchen hingegen nur sehr kurz auf. Die im letzten Teil befindlichen Workshops lesen sich zum Teil wie hilfreiche How-to-Anleitungen aus dem Internet.

Fazit

Wer viel Literatur zu einem Thema liest, neigt zum Blättern in neuen Büchern auf der Suche nach Kapiteln, die den Wissensdurst stillen. Das vorliegende Buch eignet sich aufgrund seiner Struktur ausgezeichnet zum thematischen Blättern. Nicht jedes Kapitel sticht durch Einfachheit in der Beschreibung heraus, da manchmal zu viele Informationen untergebracht werden sollen. Erfreulich, dass trotz des gewaltigen Umfangs von über 920 Seiten das Buch aufgrund seiner Bindung ohne Hardcover aufgeschlagen liegen bleibt und so hilfreich zur Seite stehen kann.

Frank Große

Autoren	Arnold Willemer
Verlag	Galileo Computing
Preis	39,90 Euro
ISBN	978-3-8362-1653-1
Bewertung *(max. 10 Punkte)*	**7**

http://msunified.net/

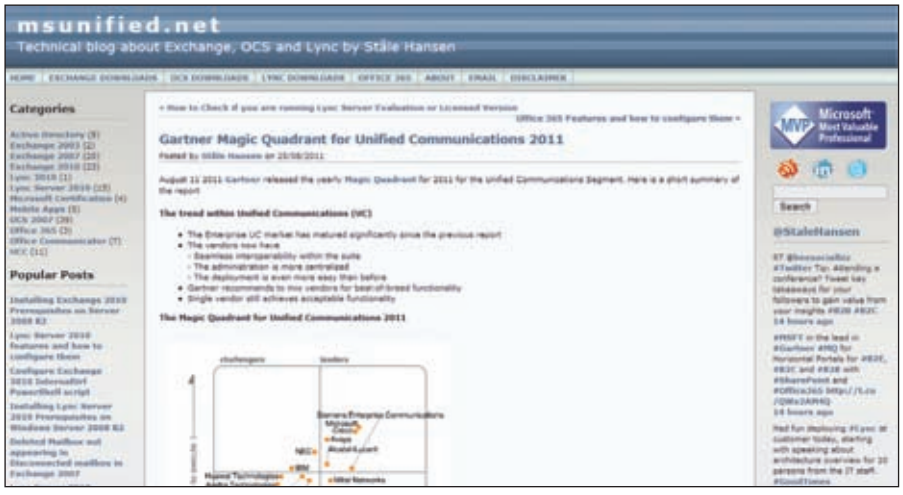
Unified Blogging

Trotz aller technischen Fortschritte ist im Umfeld von Unified Communica-tions noch immer eine der Hauptaufgaben des IT-Verantwortlichen, dafür Sorge zu tragen, dass die gemeinsam genutzten Komponenten auch gemeinsam ihren Dienst tun. Dass dies nicht immer einfach ist, dem wird sicher jeder beipflichten, der die klassischen Kommunikationskanäle Telefon, Fax und Internet bereits zusammengeführt hat und nun unter IP betreibt. Seien es nun Unwägbarkeiten bei NAT und VoIP, Fax over IP oder schlicht das unzureichende Zusammenspiel verschiedener Management-Konsolen – der Teufel steckt oft in den Details der "Zusammenarbeit".

So kann sich grundsätzlich schon einmal jeder Admin glücklich schätzen, wenn er seine Unified Communications-Infrastruktur zumindest Server-seitig mit Werkzeugen eines einzigen Herstellers betreiben kann. Sollte dieser Hersteller Microsoft heißen, so bietet Stale Hansen in seinem Blog auf msunified.net einen Rundumblick auf das Zusammenspiel von Exchange, Lync, Office Communication Server und mittlerweile auch Office 365. Hansen ist Microsoft MVP für Lync und betreibt seinen Blog seit April 2009. Er ist in Norwegen als Berater und Architekt für Unified Communications-Infrastrukturen tätig und beschreibt seinen Blog als "Sammlung wichtiger Dinge", die er nicht als private Link-Sammlung hortet, sondern allen Interessierten im Web bereitstellt.

So ist denn der Hauptnutzen für den Leser auch weniger in Hansens regulären Blog-Einträgen zu finden als auf den Seiten, die er mit "Download" bezeichnet und von denen es je eine zu Exchange, Lync und OCS gibt (und eine für Office 365 – nur hier ohne das Tag "Download"). Seine Blog-Posts zu den einzelnen Systemen sind zwar von großer technischer Tiefe, doch sind es in der Gesamtheit (noch) zu wenige, um ein so umfassendes Kompendium zu bieten wie beispielsweise Frank Carius' msxfaq.de. Hansens Stärke liegt neben der erwähnten Betrachtung des kompletten Konstrukts Unified Communications in der Vollständigkeit aller Ressourcen in seinen Beiträgen. Wer etwa den aktuell populärsten Artikel "Installing Exchange 2010 Prerequisites on Server 2008 R2" ansurft, erhält neben einer knackig-kurzen Schritt-für-Schritt-Anleitung eine komplette Linksammlung zu den zusätzlich benötigten Ressourcen wie etwa Patches oder Detailanleitungen.

Unter den Download-Reitern findet der Admin schließlich einen umfassenden Werkzeugkasten für das gewählte Produkt. Für Exchange etwa listet Hansen sozusagen chronologisch nach dem Vorgehen von Installation bis Betrieb geordnet eine Aufstellung wichtiger Tools, Whitepapers und Anleitungen auf. Auch hierbei behält er stets das große Ganze im Auge und stellt auch Hinweise von Drittanbietern bereit, etwa für den Betrieb von Exchange auf NetApp-Geräten oder unter VMware. *(jp)*



Pfade durch den Dschungel von Unified Communications bietet msunified.net

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

Das muss ein Monitoring-Werkzeug mitbringen

Um den Gesundheitszustand der immer umfassender werdenden IT-Landschaft im Auge zu behalten, muss ein Monitoring-System Flexibilität bieten, komplexe Strukturen verwalten und dennoch im alltäglichen Einsatz handhabbar bleiben. Für den Administrator ist es essenziell, stets ein vollständiges und aktuelles Bild des Ist-Zustandes seiner IT zu erhalten. Besonders KMUs mit knapp bemessenen Ressourcen fehlt bei der Wahl einer geeigneten Monitoring-Lösung aber oft die nötige Zeit. In unserem Fachartikel im Web erläutern wir, warum sich eine Überwachungs-Software schon bei Inbetriebnahme und Konfiguration beweisen muss und gehen zudem darauf ein, wie sich die Visualisierung und der Zugriff auf die Monitoring-Daten im optimalen Fall gestalten sollte.
Link-Code: BBW51

Datenflusskontrolle durch Data Loss Prevention

Jedes Unternehmen erzeugt täglich Daten, die für einen reibungslosen Betriebsablauf notwendig sind. Ein Teil dieser Daten erfordert einen besonderen Schutz: So gelten Finanzdaten, Strategien und Produktionsdetails als die Kronjuwelen eines Betriebs. Sie sind nicht nur Ziel von Spionage und Angriffen, sondern können auch durch falsche Handhabung und aus Versehen aus dem Unternehmen abfließen – Lösungen zur Data Loss Prevention leisten hier Abhilfe. Ein DLP-System überprüft bei der Verarbeitung sensibler Daten ständig, ob der Umgang den gesetzten Sicherheitsrichtlinien entspricht. Unser Online-Beitrag zeigt, wie IT-Verantwortliche die Kontrolle des Datenflusses durchsetzen, ohne dabei den produktiven Betrieb zu beeinträchtigen.
Link-Code: BBW52

Lasttests richtig aufsetzen und optimal auswerten

Mobile Apps, Rich Internet sowie Flash- und Push-Technologien verändern das Gesicht moderner Web-Auftritte. Wenn sich nach Implementierung aktueller Web 2.0-Anwendungen lange Antwortzeiten und DNS-Meldungen häufen, werden vorschnell häufig das WAN, unzureichende Hardwarekapazitäten oder Softwarefehler verantwortlich gemacht. Will der IT-Beauftragte jedoch genau wissen, was bei der Verarbeitung von Nutzeranfragen auf den Servern passiert, sind Lasttests ein unverzichtbares Diagnose-Tool zur Prävention, SLA-Absicherung oder zum Krisenmanagement. Mit künstlich generierten, hoch skalierbaren Zugriffen zeigen virtuelle Nutzer Verhalten und Verfügbarkeit der Applikationen unter Last. Wie das geht, zeigt der Fachartikel auf unserer Webseite.
Link-Code: BBW53

Besser informiert: Fachartikel auf der Website des IT-Administrator

»Im Team knacken wir auch komplexe IT-Probleme«

Gemeinsam mit seinem Co-Administrator Uwe Konopasek betreut IT-Leiter Oliver Portz (46) die gesamte IT-Infrastruktur der b.com Computer AG, sowohl am Hauptsitz in Köln als auch in den angeschlossenen deutschen Vertriebsbüros sowie der Niederlassung in Spanien. Das Unternehmen zählt zu den Vollsortimentern am deutschen IT-Distributionsmarkt und beliefert rund 13.500 Kunden.

Geburtstag: 10. Juli 1965
Admin seit: 12 Jahren
Hobbys: Reisen, Sport, Fotografie

Oliver Portz, IT-Administrator

Ausbildung und Tätigkeit

- Studium der Elektrotechnik
- Heute Leiter der IT-Abteilung

Betreute Umgebung

- Microsoft Active Directory-Netzwerk
- Apple Open Directory-Umgebung
- Microsoft Exchange
- Microsoft SQL und OpenSQL-Datenbanken und -Anwendungen
- Rund 250 Server sowie zahlreiche Netzwerkkomponenten

Wie haben sich die Anforderungen im Bereich Systemsicherheit in den letzten Jahren geändert?

Die Anforderungen sind in Quantität und Qualität gewachsen und breiter gefächert als in der Vergangenheit. Die vor allem von wirtschaftlichen Interessen getriebene Cyberkriminalität nimmt zu und die Attacken werden immer raffinierter. Der Schutz der eigenen Daten und Informationen muss für die Unternehmen im Mittelpunkt stehen. Der Einsatz neuer Technologien – so zum Beispiel im Bereich Mobile Computing – birgt oft potentielle Sicherheitsrisiken, die erkannt und umgangen werden müssen.

Welche Rolle spielen mobile Endgeräte in Ihrem Unternehmen?

Viele unserer Mitarbeiter möchten die firmeninterne IT-Infrastruktur samt unternehmensrelevanter Daten und Anwendungen auf mobilen Endgeräten nutzen. Neben klassischen Notebooks werden vermehrt auch Tablets und Smartphones in vollem Umfang bei maximaler Sicherheit eingesetzt.

Wie sichern und administrieren Sie mobile Devices?

Wir setzen in diesem Bereich momentan auf SSL VPN-Lösungen von McAfee und Juniper Networks.

Stellt Terminal Server-based Computing eine Alternative für mehr Sicherheit für Sie dar?

Ja, das wird bei uns in speziellen sicherheitssensiblen Bereichen bereits seit einiger Zeit praktiziert.

Nutzen Sie ähnliche Sicherheits-Produkte wie in der Firma auch privat?

Ja, durchaus. Die jeweiligen Consumer-Versionen von Herstellern, deren Enterprise-Lösungen sich in meinen Augen bewährt haben, nutze ich gerne im privaten Bereich, etwa zur Absicherung meines Smartphones.

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

Ja, ich würde lügen, wenn ich etwas anderes behaupten würde. Das gilt aber für das gesamte Administrationsteam. Wenn etwas Dringendes ansteht, dann beschäftigt uns das durchaus auch über die normale Arbeitszeit hinaus. Aber für Urlaub haben wir sehr klare Stellvertretungsregeln und bemühen uns, diese einzuhalten.

Wie finden Sie den nötigen Ausgleich zu Ihrer Arbeit?

Sport ist wichtig, um abzuschalten und den Akku wieder aufzuladen. Ich mag neben normalem Ausdauertraining auch Motorsport und Bowling – das fördert die Konzentration. Mein Kollege Uwe Konopasek ist da noch vielseitiger. Er powert sich gerne bei Fußball, Squash, Badminton oder Wassersport aus.

Welche Aspekte Ihres Berufs machen Ihnen am meisten Spaß und welche weniger?

Zu den angenehmen Dingen zählt sicherlich die konstruktive Arbeit in unserem tollen Administrations-Team. Spaß machen auch der tägliche Umgang mit den Menschen vor den Maschinen sowie das Erarbeiten von Konzepten und Lösungen zur strukturellen Weiterentwicklung des Unternehmens. Es gibt immer neue Herausforderungen und eine Vielfalt an Aufgaben. Der Beruf ist definitiv abwechslungsreich. Schwierige Aspekte sind hingegen der hohe Zeitdruck, der vielen Projekten zugrunde liegt, und die häufig ungewöhnlichen Arbeitszeiten.

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

Es ist ein abwechslungsreicher und moderner Beruf mit Zukunftsperspektive. Man braucht aber eine starke Affinität zur Informationstechnologie und sollte auch am Umgang mit den Menschen vor der Maschine Spaß haben.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Aktuell nehmen wir einen umfangreichen, sukzessiven Plattformwechsel von Macintosh zu Microsoft vor. Ein spannendes Projekt, das uns viel abverlangt. Daneben beschäftigen uns die kontinuierliche Weiterentwicklung der bestehenden Infrastruktur und die Verschmelzung der Kommunikationstechnologien. Darüber hinaus treiben wir die Virtualisierung von Servern und Desktops voran.

Wie denken Sie, arbeitet ein Administrator in zehn Jahren?

Das ist schwer abzuschätzen. Die Veränderungen in der IT sind im Enterprise-Bereich rasant. Wer hätte vor zehn Jahren ganz selbstverständlich über Consumerization of IT, Bring your own Device oder Cloud Computing nachgedacht? Aber definitiv ist der Beruf eines IT-Administrators von Zukunft. Ich glaube allerdings nicht, dass die Arbeitsbelastung weniger werden wird.

Das Interview führte Petra Adamik.

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

Was haben Sie zu sagen?

Die Ausgabe 1/12 erscheint am 5. Januar 2012

Schwerpunktthema:

Client-Management

Im Test: Deskcenter Management Suite

Im Test: AppSense Application Manager

Workshop: Small Business Server 2011 Essentials

Systeme: System Center Configuration Manager 2012

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

Die Ausgabe im **Februar** richtet ihren Fokus auf das Thema **Monitoring**. In unserer Test-Rubrik nehmen wir unter anderem WhatsUpGold v15 sowie den SSC-Server-Inspector in Augenschein. In unserer Praxisrubrik erfahren Sie außerdem, wie Sie Log-Dateien auf Windows-Systemen auswerten.

Als Schwerpunkt im **März** geht es dann um das Thema **Netzwerkmanagement**.

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

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

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

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

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

Autoren dieser Ausgabe
Petra Adamik, Thomas Bär, Peter Böhret, Oliver Fischer, Thomas Gronenwald, Frank Große, Mathias Hein, Jürgen Heyer, Klaus Jetter, Thomas Joos, Christian Knermann, Sandro Luciforo, Rolf Masuch, Dr. Holger Reibold, Thorsten Scherf, Isabell Unseld

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

Es gilt die Anzeigenpreisliste Nr. 8 vom 01.01.2011

LAC/2011

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

Vertriebsbetreuung
SI special interest Pressevertrieb GmbH,
www.specialinterest.com

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

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

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

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

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

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

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

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

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

INSERENTENVERZEICHNIS

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

LANCOM. Connecting your business.

Zukunftssicher:
Die neue Leistungsklasse für Ihre Unternehmenskommunikation.

Business-VPN-Router
mit hochperformantem SFP-Glasfaser-Uplink

LANCOM 1781EF

Die neuentwickelte Hardware-Plattform mit modernster CPU-Architektur und mehr Arbeitsspeicher macht Router von LANCOM jetzt noch leistungsfähiger und energieeffizienter.

- VPN-Router mit steckbarem FO-Transceiver zur WAN-Kopplung, Gigabit-Ports und 4-fach WAN-Loadbalancing
- Deutsche Firewall-Technologie (objektorientierte Stateful-Inspection, Intrusion Detection, Schutz vor DoS-Attacken)
- Hochverfügbarkeit durch ISDN und optionales UMTS-Backup (HSPA+)
- Drei Jahre Herstellergarantie

Made in Germany

IHRE MÖGLICHKEITEN

- Sichere Vernetzung von Filialen, Home-Offices und mobilen Mitarbeitern
- Übersicht und Kontrolle durch Remote Monitoring und Benachrichtigungsfunktion

IHRE VORTEILE

- Zukunftssichere Hardware-Basis mit modernster Technologie und großzügiger Speicherausstattung
- Leistungsstarker Gigabit-Ethernet-Switch mit hoher Energieeffizienz

DIE LANCOM VORTEILE

- Hohe Flexibilität und Sicherheit durch Entwicklung und Fertigung in Deutschland
- Hohe Bedienerfreundlichkeit und minimaler Schulungsaufwand durch einheitliches Management aller LANCOM Produkte

Zukunftssicher mit **Hardware 2.0**

- **Leistungsstarke CPU** mit Hardware-Zufallszahlen-Generator
- **Mehr Arbeitsspeicher** garantiert lange Nutzungsdauer
- **Energieeffizientes Gigabit-Ethernet** mit optionalem Glasfaserport

Informieren Sie sich jetzt unter:
www.lancom.de/newgeneration

1781A-3G WLAN VPN-Router mit ADSL2+ Modem
Multimodefähig Annex J/M, UMTS-Modem (UMTS / HSPA+)

1781A VPN-Router mit ADSL2+ Modem.
Multimodefähig für die neuen DSL-Standards nach Annex J/M.

LANCOM Systems