IT-ADMINISTRATOR.DE

07/2012

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

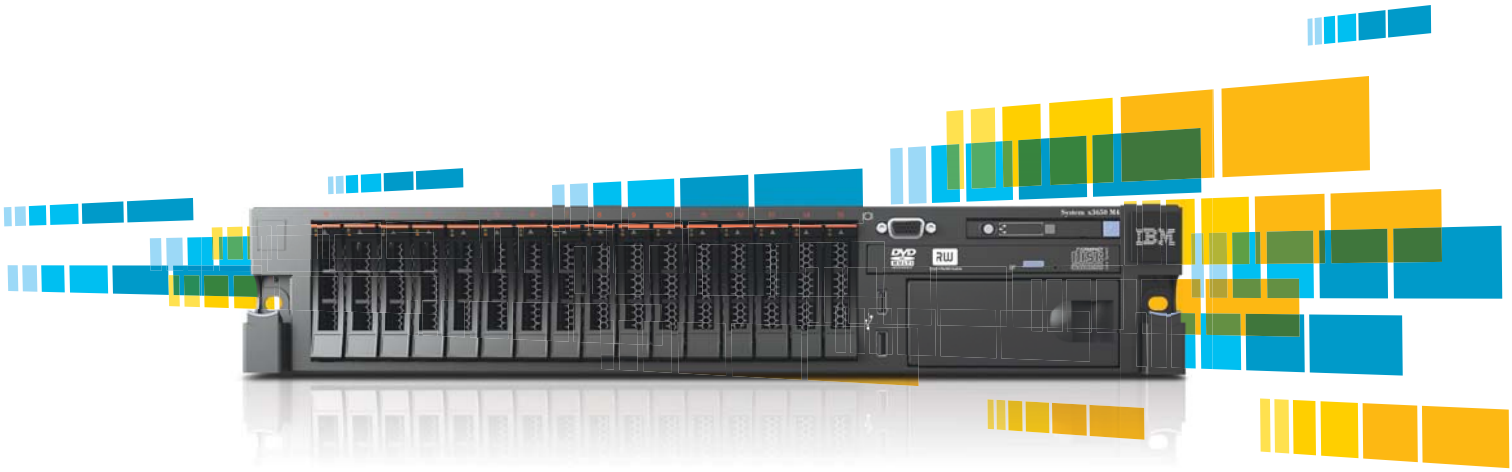
Endpoint & mobile Security

4 196583 212605 07

Gerüstet für heute. Bereit für morgen.
Der neue IBM System x3650 M4 Express Server.

Das Wichtigste für das Wachstum eines Unternehmens: eine optimierte IT-Umgebung. Deshalb ist der neue IBM System x® 3650 M4 Express Server mit den neuesten Intel® Xeon® Prozessoren der E5-2600er Serie die perfekte Plattform für Ihre zentralen Geschäftsanwendungen. Er ist nicht nur marktführend in puncto Zuverlässigkeit[1], sondern bietet bis zu 80 % mehr Rechenleistung[2], bis zu viermal mehr Arbeitsspeicher[3] und eine höhere Netzwerkbandbreite[4] als 2-Socket-Systeme der Vorgängergeneration. Und zusammen mit dem Expertenwissen der IBM Geschäftspartner erhalten Sie eine IT-Umgebung, die für Wachstum und Erfolg in Ihrem Unternehmen sorgt.

Heute schon arbeiten wie morgen. Mit den neuen IBM System x Servern.



IBM System x3650 M4 Express

2.701,– € (inkl. MwSt.)*
monatl. IBM Leasingrate: 74,55 € (inkl. MwSt.)**

Best.-Nr.: 7915E2G
Intel® Xeon® Prozessor E5-2620
1x 8 GB RDIMM-Hauptspeicher
2x 300 GB 10K 2,5" HS SAS, RAID Controller M5110e (no battery)
2x 550 W HS Power Supply, Multiburner
1 Jahr Gewährleistung, 3 Jahre freiwilliger Herstellerservice

IBM System x3550 M4 Express

2.094,– € (inkl. MwSt.)*
monatl. IBM Leasingrate: 57,79 € (inkl. MwSt.)**

Best.-Nr.: 7914E3G
Intel® Xeon® Prozessor E5-2620
1x 8 GB RDIMM-Hauptspeicher
Open Bay, 2,5" HS SAS/SATA, RAID Controller M5110 (no battery)
1x 550 W HS Power Supply, Multiburner
1 Jahr Gewährleistung, 3 Jahre freiwilliger Herstellerservice

IBM System Storage® DS3524 Express

6.296,– € (inkl. MwSt.)*
monatliche IBM Leasingrate: 167,47 € (inkl. MwSt.)**

Best.-Nr.: 1746A4D, 49Y1836
6-Gbps-SAS-Schnittstellen, optional 8-GB-FC-Anschluss
Dual Controller fasst bis zu 24 Festplatten
1 Jahr Gewährleistung, 3 Jahre freiwilliger Herstellerservice
Plus: 8x 300 GB Hot-Swap-fähige 2,5"-SAS-Festplatten

Trade-In-Programm für IBM Express Seller:
Neuen Server kaufen – Altgerät in Zahlung geben.

Bei welchen Geschäftspartnern Sie die IBM Express Seller Produkte direkt bestellen können, erfahren Sie unter **ibm.com/systems/de/express1**

[1]TBR Report: "IBM System x® x86 servers: Meeting the demands of today's enterprises by combining value and support," January 2012.
[2]Quelle: Intel-Leistungsvergleich mit SPECfp*_rate_base2006 Benchmark. Ausgangswert von 267 mit 2S Intel® Xeon® Prozessor X5690 (3,46 GHz, 6 Kerne, 12 MB L3, 6,4 GT/s, 130 W) der letzten Generation, veröffentlicht auf www.spec.org am 6.9.2011. Geschätzter neuer Wert von 486 mit 2S Intel® Xeon® Prozessor E5-2690 (2,90 GHz, 8 Kerne, 20 MB L3, 8,0 GT/s, 135 W), basierend auf Intel-eigenen Messungen vom 6.9.2011 mit zwei Intel® Xeon® Prozessoren E5-2690, Turbo aktiviert, EIST aktiviert, Hyper-Threading aktiviert, 64 GB Arbeitsspeicher (8x 8 GB DDR3-1600), Red Hat* Enterprise Linux Server 6.1 Beta für x86_6, Intel® Compiler 12.1.
[3]x3650 M4 unterstützt bis zu 768 GB Arbeitsspeicher mit 32-GB-LRDIMMs in 24 Speichersteckplätzen. Die Vorgängergeneration x3650 M3 unterstützt maximal 192 GB Arbeitsspeicher.
[4]Standardausstattung vier 1-GBit/s-Ethernetanschlüsse. Unterstützt integriertes 10-GBit/s-Ethernet mit Virtual Fabric (ohne Steckplatzbelegung). Server der Vorgängergeneration bietet zwei 1-GBit/s-Ethernetanschlüsse. Für 10-GBit/s-Ethernet muss ein PCI Express-Steckplatz belegt werden.
*Alle Preise sind Einzelhandelsverkaufspreise von IBM, gültig ab 1. April 2012. Die Preise können je nach Konfiguration schwanken. Die Einzelhändler legen ihre eigenen Preise fest, daher können die Wiederverkaufspreise an die Endverbraucher schwanken. Produkte unterliegen der Verfügbarkeit. Die Preise können ohne vorherige Mitteilung geändert werden. Es kann sein, dass im Einstiegspreis Festplatte, Betriebssystem oder andere Elemente nicht enthalten sind. Wenn Sie am aktuellsten Preis in Ihrem geografischen Gebiet interessiert sind, setzen Sie sich bitte mit Ihrem IBM Ansprechpartner oder Ihrem IBM Geschäftspartner in Verbindung.
**Monatliche IBM Leasingrate inkl. MwSt., bei 36 Monaten Laufzeit und einem Vertragsvolumen von mind. 4.000 Euro. Die Finanzierungsangebote sind freibleibend, gelten vorbehaltlich einer positiven Bonitätsprüfung durch IBM und richten sich ausschließlich an Geschäftskunden. IBM Gewährleistungsregelung zu den aufgeführten IBM System x Produkten: 1 Jahr Gewährleistung, 3 Jahre freiwilliger Herstellerservice. Die Bedingungen dieses freiwilligen Herstellerservice liegen der Lieferung bei bzw. sind unter ibm.com/servers/support/machine_warranties abrufbar. Die Gewährleistung gemäß den Geschäftsbedingungen der IBM, insbesondere die Gewährleistungsfrist von zwölf Monaten, bleibt davon unberührt.

EDITORIAL

Tarnen und Täuschen

Liebe Leser,

wissen Sie, was erfolgreiche Malware mit vielen Tierarten verbindet? Eines der Grundprinzipien für das eigene Überleben. Flame heißt der jüngste Superschädling, der perfekt getarnt sein Unwesen treiben konnte. Da musste auch Mikko Hypponen, Chef-Virenforscher bei F-Secure, das Versagen seiner Zunft einräumen. Flame flog nämlich aufgrund der geringen Verbreitung und des geschickt geschriebenen Codes unter dem Radar der Erkennungsautomatik in den Virenlabors. Besonders perfide: Mit einem gefälschten Microsoft-Zertifikat im Gepäck täuschte Flame ein legitimes Windows-Update vor. Das dürfte selbst erfahrene Nutzer endgültig hinters Licht geführt haben. Doch ob der Unmenge an täglich neuem Schadcode haben die Virenjäger gar keine andere Wahl, als ihre Analyse zu automatisieren. Ein Ansatz, der unter IT-Sicherheitsexperten inzwischen Kritik hervorruft.

Was bedeutet das für Sie als Administrator? Vor allem dürfen Sie nicht bereits nach dem Antivirus-Rollout auf (mobilen) Endgeräten den Punkt "Sicherheit" abhaken. Vielmehr tragen auch Konzepte wie die Desktop- und Applikations-Virtualisierung ihren Teil bei. Mit dieser schaffen Sie getrennte Umgebungen für Privates und Geschäftliches oder für vertrauliche und unkritische Firmendaten. Zusätzlichen Schutz bietet die strikte Kontrolle von Anwendungen auf Clients ebenso wie ein durchdachtes Identity- und Log-Management. Und natürlich dürfen Sie die Datenverschlüsselung und das Patchmanagement nicht vergessen. Ergo: Jede Menge Arbeit bei begrenzten IT-Budgets und mangelnder Zeit!

Um Ihnen einige Mittel für mehr Sicherheit an die Hand zu geben, erfahren Sie ab Seite 32, was Endpoint Security heute leisten muss. Außerdem zeigen wir Ihnen ab Seite 54, wie Sie die Zugriffe mobiler Anwender auf Ihr Firmennetz absichern. Ein Update zur Sicherheit unter dem brandneuen Windows 8 erhalten Sie ab Seite 62. Bleibt zum Schluss noch die rechtliche Betrachtung der IT-Sicherheit, die wir Ihnen ab Seite 68 näher bringen. Nicht, dass aus einem Sicherheits-Fauxpas auch noch ein juristisches Fiasko entsteht.

Viel Spaß beim Lesen,
Ihr

Daniel Richey
Stellv. Chefredakteur

PS: Noch bis 6. Juli können Sie an unserer Leserumfrage zum Tool des Jahres 2012 teilnehmen und wertvolle Preise gewinnen. Machen Sie noch heute mit unter Link-Code PDJ12.

Endpoint & mobile Security

Im Test: LogMeIn Hamachi 2.1

Die zunehmende Mobilität der Mitarbeiter verlangt nach einer sicheren Lösung für eine Internet-weite Vernetzung. Statt dazu mit hohem Aufwand eigene VPN-Technik zu unterhalten, bietet sich als preisgünstige Alternative der Netzwerkvirtualisierungsdienst Hamachi von LogMeIn an. IT-Administrator hat sich das Angebot besonders hinsichtlich Flexibilität und Sicherheit einmal genauer angesehen.

Seite 18

Anwendungen unter Windows mit Applocker kontrollieren

In Windows 7 können Anwender auch ohne Administratorrechte Programme installieren. Auch das direkte Starten von Anwendungen über ausführbare Dateien ist problemlos möglich – ein Einfallstor für unsichere Software oder verseuchte Anwendungen. Applocker soll Administratoren ein Beschränken des Anwendungszoos auf Clients ermöglichen. Ein weiterer Nutzen liegt im Sperren nicht lizenzierter Anwendungen. Die Funktion ist lokal verfügbar und lässt sich auch über Gruppenrichtlinien steuern. Wie das geht, lesen Sie in unserem Workshop.

Seite 42

Mobile Geräte an Microsoft-Infrastrukturen anbinden

Erst die Anbindung an die Ressourcen und Daten im Unternehmen macht aus einem Smartphone oder Tablet ein vollwertiges Arbeitsmittel. Intern muss der Zugriff durch Geräte-Richtlinien gestaltet werden. Erfolgt dieser von außen, bietet sich ein VPN an. In einer Microsoft-basierten Infrastruktur benötigt der mobile Client zusätzlich den Zugriff auf Exchange und SharePoint. Wie und mit welchen Zusatztools Administratoren diese Anforderungen umsetzen, zeigt der Workshop.

Seite 54

Aktuelle Trends und Entwicklungen bei Public Key-Infrastrukturen

PKI gibt sein Comeback im großen Stil: Da immer mehr Web- und Cloud-Dienste ihre Authentifizierung auf Zertifikate aufbauen und Letztere insbesondere auch für mobile Geräte an Bedeutung gewinnen, sehen sich IT-Verantwortliche zunehmend mit dem Bedarf einer Public Key Infrastructure konfrontiert. Im Fachartikel beschreiben wir die Komponenten einer PKI, geben Einblicke darüber, wie sich eine PKI im Eigenbetrieb sichern lässt und zeigen anhand aktueller Anwendungsszenarien die praktische Umsetzung.

Seite 72

Link-Codes

Unsere Link-Codes ersparen Ihnen mühsame Tipparbeit bei langen URLs

Power-Management im großen Stil

Emerson Network Power stellt die **Trellis-Plattform** zur Überwachung der **IT- und Facility-Infrastuktur** vor. Damit sollen IT-Verantwortliche einen integrierten Überblick über ihr Rechenzentrum erhalten und den Strom- sowie Kühlungsbedarf zielgenauer planen können. Der Trellis Inventory Manager stellt dabei die Grundlage für ein **Modell der Rechenzentren** dar, informiert die Nutzer über den Standort von Geräten und Ausrüstung, veranschaulicht die Beziehung zwischen diesen Komponenten und zeigt die von der Rechenzentrumsausrüstung beanspruchten Ressourcen. Der Site Manager meldet den **Zustand der Infrastruktur** einschließlich Umgebungsbedingungen. Der Change Planner arbeitet mit Inventory Manager zusammen, um die **Nutzung genauer und einheitlicher Informationen zu gewährleisten**. Dies soll sicherstellen, dass Installationen, Umlagerungen und Stilllegungen von Ausrüstung und Geräten einheitlich geplant, nachverfolgt und die entsprechenden Informationen an Teammitglieder weitergeleitet werden. Die Funktion Energy Insight berechnet den **Energieverbrauch im Rechenzentrum**, die Stromkosten sowie den Wert für die Effektivität der Energienutzung (Power Usage Effectiveness, PUE) sowie die Effizienz von Rechenzentrumsinfrastrukturen (Data Center Infrastructure Efficiency, DCiE). Der Plattform-Server kostet 5.000 Euro, die Module rund 10.000 Euro. Die zugehörige Appliance, die neben der Trellis-Funktion auch KVM ermöglicht, kostet ab 9.000 Euro. Zudem sind die eingebundenen Geräte ebenfalls zu lizenzieren. *(dr)*

Emerson Network Power: www.emersonnetworkpower.com

Alle unter einem Dach

Aagon Consulting bringt die im Frühjahr vorgestellte **Version 3.8.10 von ACMP** nun offiziell auf den Markt. Die Software inventarisiert neben Windows-PCs jetzt auch die Hard- und Software von Arbeitsplatzrechnern unter **Mac OS X und Linux**. Zudem unterstützt ACMP ab sofort Administratoren bei der automatisierten Verteilung von Software auf allen drei Plattformen. Dabei arbeitet der ACMP-Agent eng mit den jeweiligen Paketmanagern der Betriebssysteme zusammen. Die zentrale Schaltstelle zur Verwaltung aller Client-PCs im Unternehmen bleibt weiterhin die **ACMP-Konsole**. Dort finden sich jetzt zwei neue Optionen im Package-Wizard, die Administratoren bei der Verteilung von Softwarepaketen für Mac OS und Linux unterstützen. Findet ACMP einen Apple-Rechner oder Linux-PC, so installiert die Clientmanagement-Software dort automatisch ihren Agenten und startet im Anschluss auf Wunsch einen ersten Inventarisierungslauf. Einzige Voraussetzung für die Installation von ACMP auf Mac- und Linux-Clients ist ein aktiver SSH-Zugang. Windows-PCs hingegen übernimmt ACMP automatisch aus dem Active Directory und installiert dort seine Agenten per Push-Installation oder über Gruppenrichtlinien. Des Weiteren hat Aagon den ACMP-Helpdesk um CTI-Funktionen und ein neues Benachrichtigungsmodul erweitert. So informiert jetzt ein Helpdesk-Notifier den Benutzer über das System-Tray seines Windows-PCs über neue Trouble-Tickets, die Eskalation offener Tickets oder sonstige Ereignisse im Support-System. Der ACMP-Server läuft unter Windows Server 2000, 2003, 2008 und 2008 R2. Eine Clientlizenz von ACMP 3.8.10 kostet je nach Abnahmemenge zwischen 39 und 65 Euro. *(dr)*

Aagon Consulting: www.aagon.de

Auto Tiering für Einsteiger

NetApp baut seine Produktfamilie an Storage-Systemen um das Einstiegsmodell **FAS2220** aus. Die Speicherkomponente verwendet die neue **NetApp Flash Pool Technologie**. Diese ermöglicht ein **automatisches Tiering** zwischen SATA- und SSD-Platten und soll so die Applikations-Performance deutlich erhöhen. Das Gerät misst zwei Höheneinheiten und bietet Platz für bis zu zwölf Platten. Maximal unterstützt die Neuerscheinung 180 TByte auf 60 Festplatten. Bis zu acht Ethernet-Ports und vier Onboard SAS-Anschlüsse stellen die Verbindung zum Netzwerk her. Anders als das nächstgrößte Modell der Serie, das FAS2240, unterstützt der kleinere Bruder weder 8 GBit-Fibre Channel noch 10 GBit-Ethernet. Als Übertragungsprotokolle beziehungsweise Dateisysteme kommen iSCSI, NFS, CIFS zum Einsatz. Der mit der Storage-Komponente ausgelieferte NetApp OnCommand System Manager 2.1 soll die Einrichtung und das laufende Management von Geräten des Herstellers vereinfachen. Die FAS2200-Serie läuft unter der aktuellen Version des Betriebssystems Data ONTAP. Kunden erhalten damit laut NetApp eine skalierbare Unified Architecture, mit der sie ihre Systeme einfach und kostengünstig aufrüsten, neue Funktionen ergänzen sowie aufwändige Upgrades vermeiden. Data ONTAP sei zudem clusterfähig, so dass mittelständische Unternehmen ihren Infrastrukturen nach Bedarf und ohne Ausfallzeiten weitere Storage-Kapazitäten hinzufügen könnten. Das FAS2220 ist ab sofort ab 6.600 Euro erhältlich. *(ln)*

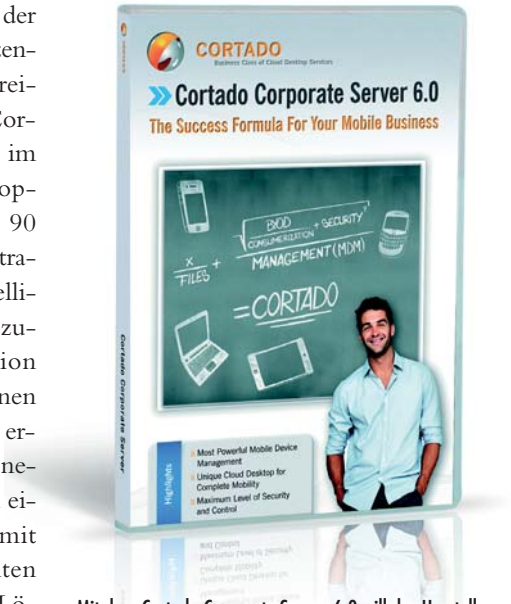
NetApp: www.netapp.com/de/

Auch für Storage-Einsteiger bietet die Speicherlösung FAS2200 vollen SSD-Support

Mobile Device Manager mit Desktop-Funktion

Cortado feuert mit **Corporate Server 6.0** den Startschuss für die neueste Version seiner **Software zum Mobile Device Management** (MDM) ab. Das neue Release erlaubt die **Verwaltung von iPhone und iPad sowie Android- und BlackBerry-Smartphones** und bietet dem Nutzer laut Hersteller vollständige Desktop-Funktionalitäten inklusive Direktzugriff auf das Dateisystem des Unternehmens. Der Dokumentenzugriff erfolgt dabei auf Basis der bereits bestehenden Active-Directory-Rechte des Anwenders – alle sicherheitsrelevanten Aspekte von mobilen Endgeräten soll der Administrator so von einer Stelle aus zentral überwachen können. Trotz weitreichender Zugriffsoptionen wird laut Cortado bei der Nutzung des Werkzeugs im Vergleich zu anderen Cloud-Desktop- oder File-Sharing-Lösungen bis zu 90 Prozent weniger Datenvolumen übertragen. Dies sei unter anderem auf intelligente Komprimierungsalgorithmen zurückzuführen, eine Preview-Funktion sowie die Möglichkeit, Dateioperationen serverseitig auszuführen. Die Software ermöglicht es Unternehmen weiterhin, neben einem Enterprise App Store auch einen Resource Store zu betreiben, mit dem sich Webanwendungen einrichten lassen. Als Sicherheitsmerkmale der Lösung nennt der Hersteller unter anderem den Single Point of Entry für MDM, Remote Wipe und die Protokollierung aller Aktionen des Nutzers in einem Audit Trail. Mit zum Funktionsumfang gehört außerdem eine Cloud Printing-Option. Die Lizenzierung von Cortado Corporate Server 6.0 erfolgt auf Miet- oder Kauf-Basis. Der Mietpreis beträgt etwa bei 30 Lizenzen pro Nutzer und Monat knapp 4 Euro. Der Kaufpreis für ein Basic Pack für fünf Nutzer liegt bei 795 Euro, für jeden zusätzlichen Anwender kommen 97 Euro hinzu. *(ln)*

Cortado: www.cortado.com/eude/



Mit dem Cortado Corporate Server 6.0 will der Hersteller Mobile Device Management mit sicherem Dateizugriff für den Anwender kombinieren

Remote-Support ganz nah

Citrix gibt umfassende Erweiterungen seiner **Remote-Support-Software GoToAssist** bekannt. Zu den neuen Funktionalitäten zählen zusätzliche **mobile Apps**, die Integration in mobile und soziale Arbeitsumgebungen mittels **kundeninitiierten Supports** sowie die **Integration mit Citrix Receiver-Clients**. Organisationen, die ihr Service-Portfolio um Support über Social Communities erweitern möchten, können mit GoToAssist nun direkte Anfragen aus Online-Kundendialog-Foren ermöglichen. Die Anwender können damit nahtlos vom Self-Service-Support in der Community zum Full-Service-Support wechseln. Die Integration von GoToAssist mit Citrix Receiver soll noch in diesem Jahr auf den Markt kommen. Durch eine gemeinsame Nutzung des Receivers und GoToAssist können IT-Abteilungen Live-Support direkt aus dem Receiver heraus anbieten. Endanwender haben somit die Möglichkeit, sich über einen Klick auf den GoToAssist-Support-Button mit ihrem internen Help Desk zu verbinden. Schließlich ist GoToAssist nun auch für Android als App verfügbar. Für GoToAssist Remote Support liegen die Kosten bei 49 Euro im Monat. *(dr)*

Citrix: www.gotoassist.com

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

Die United Internet-Tochter **ProfitBricks** geht mit einem **Infrastructure as a Service-Angebot** an den Start. Das Besondere dabei: Über die grafische Benutzeroberfläche "Data Center Designer" (DCD) kann der Nutzer ein komplettes virtuelles Rechenzentrum individuell zusammenstellen und per Mausklick die Konfiguration aktivieren oder beliebig ändern – egal ob es sich um Server, Storage, Loadbalancer, Firewalls oder die entsprechende Vernetzung handelt. Für jeden Server lassen sich CPU-Cores und RAM flexibel per Schieberegler zuweisen. Abgerechnet wird minutengenau nach der beanspruchten Leistung. So fallen für einen Server in Minimalkonfiguration 5 Cent je Stunde an. Jedes GByte an Traffic kostet außerdem 6 Cent. *(dr)*

www.profitbricks.de

Scendix bringt mit **PamLytics** eine Software auf den Markt, die die Nutzung von Skype im Unternehmen überwacht und dokumentiert. Dabei greift das Werkzeug auf die Skype Desktop API zurück, um sämtliche Voice- und Video-Anrufe sowie Text-Chats zu protokollieren. Hierbei erfolgt laut Hersteller keine Aufzeichnung des Inhalts – lediglich die Basisdaten wie die Gesprächsteilnehmer oder die Länge der Konversation würden festgehalten. Der Administrator kann die gesammelten Daten dann über ein Web-basiertes Portal abrufen und analysieren. Das Interface bietet dazu anpassbare Ansichten und Exportfunktionen. Die Lizenzierung erfolgt auf Subskriptions-Basis – je nach Anzahl der verwalteten Nutzer kostet PamLytics pro User mindestens 3,50 Euro. *(ln)*

www.pamlytics.com

Mit **harmon.ie Mobile for iPad** gibt **harmon.ie** die Verfügbarkeit seiner Software zur Integration von Office über den Microsoft Sharepoint Server bekannt. Anwender können damit Dokumente aus dem Unternehmen suchen, betrachten und editieren, aber auch mit Kollegen in Interaktion treten und Dokumente gemeinsam bearbeiten. Daneben unterstützt das Tool Collaboration und Social Networking. Zu diesen Features gehören unter anderem Activity Streams, die Facebook-Funktionen rund um die Dokumentenarbeit bieten. harmon.ie for iPad gibt es als kostenlose Lite App mit eingeschränktem Funktionsumfang und als Vollversion für 16 Euro. Für das iPhone ist eine auf den kleineren Bildschirm optimierte App erhältlich. *(ln)*

http://harmon.ie/

Mit Version 15 der Management-Software **ETERNUS SF** macht **Fujitsu** die Technologie des Automated Storage Tiering (AST) für ETERNUS DX-Speichersysteme und damit für den Einsatz im KMU-Bereich verfügbar. AST ist damit laut Fujitsu nicht mehr an die Systemgröße gebunden und soll Unternehmen dazu befähigen, Speicherkapazitäten effizienter auszunutzen. Dies geschieht über die automatische Datenspeicherung in unterschiedlichen Storage-Tiers beziehungsweise auf unterschiedlichen Festplattentypen – je nach den Vorgaben, die vom IT-Administrator getroffen wurden. Bestimmende Parameter sind beispielsweise die Systemleistungsfähigkeit, Kapazitätsanforderungen oder auch Speicherkosten. Die ETERNUS SF Management-Software steht ab sofort mit allen Plattenspeichersystemen der Serie ETERNUS DX zum Einsatz bereit. *(ln)*

www.fujitsu.com/de/

Volle Fernkontrolle

ATEN liefert ab sofort zwei neue **Dual-Rail LCD-KVM-over-IP-Switches** aus. Die IP-fähigen Kontrolleinheiten **KL1508Ai** und **KL1516Ai** mit integriertem Monitor ermöglichen den sicheren **Zugriff auf acht beziehungsweise 16 Server** über eine KVM-Konsole. Dank Slide-away-Chassis lassen sich bei beiden Modellen der integrierte LCD-Monitor, die Tastatur und das Touchpad platzsparend in das Rack zurückschieben. Über TCP/IP können Administratoren laut Hersteller von jedem Rechner im LAN, WAN oder Internet auf den KL1508Ai beziehungsweise KL1516Ai zugreifen. Die Neuerscheinungen verfügen über einen Panel Array-Modus, über den sich Videoinhalte von bis zu 16 Computern auf einem Display anzeigen lassen. Daneben bieten die IP-fähigen Konsolen eine Message Board-Funktion, die angemeldeten Benutzern die Kommunikation untereinander ermöglicht. Ausgestattet sind beide Varianten mit RJ-45-Steckern und CAT5e/6-Kabeln für eine kompakte und effiziente Kabelverbindung. Die Funktion "Maus DynaSync" synchronisiert die lokalen und Remote-Maus-Bewegungen und soll die Ausrichtung des Mauszeigers unabhängig von den Servereinstellungen optimieren. Die neuen LCD KVM-Switches sind je nach Bildschirmgröße zu Preisen zwischen 1.865 Euro und 2.110 Euro erhältlich. *(ln)*

ATEN: http://de.aten.eu

Die neuen KVM-Switches von ATEN "KL1508Ai" und "KL1516Ai" sind jeweils mit einem 17 oder 19 Zoll-Monitor ausgestattet

Einfach-NAS mit Profi-Features

LaCie bietet einen neuen **NAS-Server mit zwei Laufwerkschächten** an: das **LaCie 2big NAS**. Mit einem 2 GHz-Prozessor und einem verbesserten Dateisystem ausgestattet, soll das NAS Datentransferraten von bis zu 100 MB/s ermöglichen. Das Gerät bietet mehrere Sicherheitsstufen, einschließlich RAID 1 zur Datenspiegelung. Dank der **Hot-swap-fähigen Laufwerke** kann eine fehlerhafte Festplatte ohne Unterbrechung, ohne Datenverlust und ohne Neustart des Geräts im laufenden Betrieb ausgetauscht werden. **LaCies NAS OS 2-Dashboard** soll es Unternehmen ferner vereinfachen, das System automatisch zu sichern. Assistenten mit Voreinstellungen erledigen komplexere Aufgaben wie RAID-Management, Benutzerverwaltung und NAS-zu-NAS-Datensicherung. Benutzer können das Herunterfahren und Neustarten für die Geschäftsstunden programmieren und damit die Energieeffizienz verbessern. Darüber hinaus ist das NAS im Deep-Sleep-Modus laut Hersteller zehnmal energieeffizienter als die Vorgänger-Generation. Dank **Wake-on-LAN** können Anwender vom Deep-Sleep-Modus aus auf das NAS zugreifen. Das NAS soll so für eine komplette Datensicherung von Linux-, PC- oder Mac-Rechnern sorgen. Anwender haben die Wahl, entweder Time Machine, Windows 7 Backup oder die im Lieferumfang enthaltene LaCie-Datensicherungssoftware zu nutzen. Mit einer Speicherkapazität von 6 TByte kostet das System 537 Euro. *(dr)*

LaCie: www.lacie.com

Ermöglicht den Plattentausch im laufenden Betrieb: das LaCie 2big NAS

Access Points mit Ausstrahlung

Ruckus Wireless baut sein Angebot an **Access Points** nach oben und nach unten hin aus. Der **ZoneFlex 7982** wurde für Umgebungen mit einer hohen Nutzerdichte entwickelt und ist laut Hersteller der einzige **Dual-Band Three-Stream 802.11n-Access Point**, der mit einem **adaptiven Antennen-Array mit Dual-Polarisierung** ausgestattet ist. Dies erlaubt die gleichzeitige Nutzung der adaptiven Antennenwahl und die Beamforming-Übertragung, wodurch Verbesserungen von bis zu 9 dB bei Signal-to-Interference and Noise (SINR) und bis zu 15 dB an Interferenz-Abschwächung realisierbar sind. Der Access Point eignet sich damit etwa für Umgebungen mit hohem Datenaufkommen wie Flughäfen, Hotels und andere öffentliche Orte. Der auf der neuesten Generation des Atheros Three-Stream High-Performance Chipsatz basierende AP kann bis zu 500 Clients gleichzeitig bedienen. Der **ZoneFlex 7321** hingegen ist mit 198 Gramm besonders leicht und kompakt. Das Gerät erlaubt bis zu 256 gleichzeitige Nutzer. Der Access Point funkt im Standart 802.11n mit Dual-Band und verfügt über zahlreiche Features, wodurch er ideal für kleinere Ein-AP-Einsatzumgebungen geeignet ist, wie etwa Hotspots, KMUs und Remote-Büros. Das Gerät unterstützt dabei Beamforming-Übertragung und eine kapazitätsabhängige Kanalwahl, um eine hohe Leistung und Reichweite mit Verbesserungen von bis zu 4 dB in der Signal-Verstärkung zu gewährleisten. Sowohl der ZoneFlex 7982 als auch der 7321 ermöglichen Power-over-Ethernet und können entweder als Standalone Wireless AP mit Routing-funktionalität oder als Teil einer zentral gesteuerten Smart WLAN-Umgebung eingesetzt werden. Beide Modelle sind ab sofort zu haben. Die Preise beginnen bei 1.099 US-Dollar für den 7982 und 349 Dollar für den kleinen Bruder 7321. *(dr)*

Ruckus Wireless: www.ruckuswireless.com

Der Access Point ZoneFlex 7982 bietet eine adaptive Antennenwahl und Beamforming

An der kurzen Leine

Absolute Software will mit **Absolute Manage 6.1** den Trend zu **Bring Your Own Device** adressieren. Die Software ermöglicht nun eine **automatisierte Registrierung von Endgeräten** im Unternehmensnetzwerk. Statt sich um jedes Gerät einzeln zu kümmern, kann die IT-Abteilung einen automatisierten Prozess nutzen, um jeden Angestellten durch den Registrierungsvorgang zu lotsen. Dazu zählt auch die Vorlage einer rechtlichen Vereinbarung, der jeder Mitarbeiter zustimmen muss, um sein Gerät anmelden zu können. Darüber hinaus bietet Absolute Manage 6.1 ein **verbessertes Mobile Application Management**: Dies beinhaltet die automatische Installation oder Deinstallation von Apps – je nach Gerätestatus und Anwender. Ferner gibt es die Möglichkeit, auf Basis vorab definierter Bedingungen einzelne IT-Befehle automatisiert auszuführen. Dazu zählt unter anderem eine Roaming-Sperre, die Herabstufung eines Geräts auf den Status "nicht verwaltet", die Benachrichtigung der IT und die Übermittlung einer Nachricht an den Nutzer eines Geräts. Version 6.1 bietet zusätzlich neue Funktionen für PC und Mac, darunter einen plattformübergreifenden Zugriff aus der Ferne und die Bereitstellung von detaillierten Verschlüsselung-Statusberichten. Sowohl das Betriebssystem Android als auch iOS sind mit der Lösung gleichwertig verwaltbar. Absolute Manage 6.1 ist ab sofort verfügbar. Der Preis beginnt bei 22 Euro pro Endgerät für eine Jahreslizenz. *(dr)*

Absolute Software: www.absolute.com

Günstiges Öko-WLAN

ZyXEL stellt mit dem **NGB-419N v2** einen überarbeiteten **Wireless-N-Router mit NetUSB-Funktion** vor. Wie sein Vorgänger NBG419N arbeitet auch das neue v2 Modell mit der **802.11n-Funktechnologie** und erreicht so Übertragungsgeschwindigkeiten von bis zu 300 MBit/s. Neben dem Vier-Port-Switch können über die im neuen Modell integrierte NetUSB-Funktion USB-Geräte, wie Drucker oder NAS-System, angeschlossen werden. Um Kosten zu sparen, verfügt das Gerät über **drei Stromspar-Features**: Die einfachste und effektivste Stromspar-Methode ist durch den am Gehäuse angebrachten Ein-/Aus-Schalter erreichbar. Außerdem lässt sich die Wireless-Funktion zu bestimmten Uhrzeiten automatisch ein- oder ausschalten. Zu guter Letzt soll das Wireless Output-Management dabei helfen, den Stromverbrauch im Auge zu behalten und weiter zu reduzieren. So lässt sich der Router individuell auf das Nutzungsverhalten der Anwender einstellen. Für 46 Euro geht das Gerät über die Ladentheke. *(dr)*

ZyXEL: www.zyxel.de

Der ZyXEL-Router NGB-419N v2 bietet NetUSB und soll beim Energiesparen helfen

IT-Administrator Workshop "Windows-Terminaldienste und Citrix XenApp" in Hamburg und Düsseldorf

Terminal Services reloaded

ITANet Workshop-Partner:

von John Pardey

Lange bevor der Begriff der Virtualisierung die IT-Welt erfasste, stellten IT-Verantwortliche ihren Anwendern Arbeitsumgebungen per Terminal Services zur Verfügung. Heute nennt Microsoft diese Technik "Remote Desktop Services" und diese werden wie eh und je durch Produkte von Citrix ergänzt. Doch stellen die Terminaldienste Administratoren auch heute noch vor technische Herausforderungen – exemplarisch sei das Thema Drucken erwähnt. Unsere kostenlosen Workshops im September werfen einen Blick auf Best Practices für beide Systeme und stellen kommende Neuerungen vor.

Selbstverständlich sind aktuelle Terminalserver- und Citrix-Infrastrukturen heute nicht annähernd so fehleranfällig wie ihre Vorgänger. Doch wie fast überall in der IT weicht die große Fehleranfälligkeit einer steigenden Komplexität. Hier gilt es sorgsam zu planen und nach Best Practices zu handeln. Ziel unserer beiden kostenlosen Workshops unter der Leitung von Oliver Frank, Director Consulting bei Login Consultants – einem der führenden Beratungshäuser für Terminalserver-Technologien –, ist daher die Vermittlung aktueller Best Practices und Hilfestellung bei der praktischen Arbeit und der Fehlersuche.

Best Practices Windows-Terminaldienste

Die Windows-Terminaldienste (aktuell Remote Desktop Services genannt) bilden nach wie vor die Basis für die zentrale Bereitstellung von Anwendungen im Unternehmen. Doch aus den kleinen Installationen der ersten Stunde sind heute teilweise riesige Silos entstanden, die tausende Anwender mit Applikationen versorgen. Daraus resultiert natürlich auch eine Verschiebung bei der Verwaltung, bei der heute ein optimales Design der Infrastruktur den zentralen Punkt der Leistungsfähigkeit darstellt. Verbunden mit Best Practices der Administration bietet Dozent Oliver Frank im ersten Themenblock des Workshops Hilfestellung zum Betrieb von Terminalserver-Infrastrukturen und zeigt, wo die Bordmittel an ihre Grenzen stoßen.

Das Beste auch für XenApp

Im zweiten Abschnitt des Workshops wendet sich Frank dann nützlichen Erfahrungswerten, Designtipps und Best Practices rund um Citrix XenApp zu. XenApp unterstützt auch nach vielen Wechseln im Produktnamen weiterhin die Bereitstellung von Anwendungen durch Terminalserver, indem es beispielsweise deren Multimedia-Fähigkeiten verbessert oder zusätzliche Management-Funktionen bietet. Ergänzend erhellt unser Dozent das Zusammenspiel von Provisioning Services, Hypervisor und XenDesktop und sorgt so für ein tiefgehendes Verständnis über die Vorgänge in derartigen Infrastrukturen. Und auch nützliche Zusatz-Tools kommen nicht zu kurz.

Was die Zukunft bringt

Mit Windows Server 2012 steht eine neue Version des Serverprodukts ins Haus und damit auch Anpassungen und neue Features der Terminaldienste. Was Sie hier erwarten dürfen und welche Neuerungen bei XenApp anstehen, erfahren Sie im letzten Abschnitt des Workshops. Zudem beschäftigen wir uns hier mit Automationstools im Terminalserver-Umfeld. Wir würden uns sehr freuen, Sie zahlreich auf unseren kostenlosen Workshops begrüßen zu dürfen.

Agenda

13:00 Uhr: Begrüßung

13:15 Uhr: Windows Remote Desktop Services
- Best Practices Remote Desktop Services
- Architektur und Designtipps
- Tools und Hilfestellungen

Dozent: Oliver René Frank, Director Consulting, Login Consultants Germany GmbH

14:45 Uhr: Kaffeepause

15:00 Uhr: Partnervortrag: Anwendungsbereitstellung in LAN und WAN
- Performanter Remotezugriff mit RDP-Beschleunigung
- Terminalserver plus Anwendungsvirtualisierung – der VDI-Killer
- Sicherer Zugriff auf Unternehmensanwendungen – anywhere, any device

Dozent: Frank Buermann, Leiter NDM Vertrieb, H+H Software GmbH

15:45 Uhr: Citrix XenApp
- Best Practices XenApp
- Architektur und Designtipps
- Zusammenspiel Provisioning Services, Hypervisor und XenDesktop
- Tools und Hilfestellungen

Ausblick: Neuerungen in Windows Server 2012 und XenApp
- Neue Features in den Windows Server 2012-Terminaldiensten
- Neuerungen des kommenden XenApp-Release
- Leistungsfähige Automationstools

Dozent: Oliver René Frank

17:30 Uhr: Ende des Workshops

Termin & Ort

11. September: Hamburg

Fast Lane Institute for Knowledge Transfer GmbH, Gasstraße 4a, 22761 Hamburg

24. September: Düsseldorf

Fast Lane Institute for Knowledge Transfer GmbH, Hansaallee 249, 40549 Düsseldorf

Teilnahmegebühr

Für IT-Administrator Abonnenten kostenlos.

Sollten Sie über ein Abonnement verfügen und einen oder mehrere Kollegen zum Workshop mitbringen wollen, erheben wir eine Schutzgebühr von 75 Euro (zzgl. 19% MwSt) pro zusätzlichem Teilnehmer. Für Nicht-Abonnenten wird eine Schutzgebühr von 145 Euro (zzgl. 19% MwSt.) fällig.

Workshop "Windows-Terminaldienste und Citrix XenApp"

IT-Administrator Training "VMware Best Practice" in Frankfurt und München

Besser virtualisieren

von John Pardey

In wenigen Jahren hat sich VMware ESX beziehungsweise vSphere zu einer zentralen Komponente zahlreicher IT-Infrastrukturen entwickelt. Neben der rasanten Verbreitung des Systems nahmen mit aufsteigender Versionsnummer sowohl die Komplexität als auch die Möglichkeiten exponentiell zu. In unserem neuen Training "VMware Best Practice" in München und Frankfurt/Dietzenbach nimmt daher Virtualisierungs-Experte und IT-Administrator-Autor Dennis Zimmer das System hinsichtlich des optimalen Betriebs unter die Lupe.

Sah sich der Administrator in den Anfangstagen der Virtualisierung mit den üblichen Kinderkrankheiten einer neuen Technologie konfrontiert, blickt er heutzutage nicht selten auf eine Infrastruktur, die hochgradig virtualisiert ist. Zwar sind frühere Probleme beseitigt, doch vielfältige Management-Aufgaben warten nun auf den Administrator. Daher bilden Best Practices für diese Themen die zentralen Aspekte unseres neuen Trainings.

Plane und herrsche

Im ersten Block des Trainings stellt unser Dozent Dennis Zimmer zunächst wichtige Aspekte der Planung und der Netzwerk- sowie Storagekonfiguration in den Mittelpunkt seiner Ausführungen. Denn schon kleine Fehler in der Planung beziehungsweise der Erstkonfiguration können IT-Abteilungen im Nachhinein das Leben sehr schwer machen.

Aufbauend auf einem optimalen Gerüst wendet sich Zimmer dann Management-Aufgaben wie Sicherheit und Sicherung zu. Aber auch für virtualisierte Desktops sowie für den Betrieb der virtuellen Maschinen sowie der darin laufenden Applikationen hat Zimmer praxisnahe Empfehlungen parat. Zum Abschluss des ersten Abschnitts wirft der Dozent dann noch einen Blick darauf, was Administratoren aktuell und zukünftig von der Cloud in Sachen Management, Automatisierung und Abrechnung erwarten dürfen.

Notfall-Handbuch

Ein Tag rund um Best Practices für VMware kommt nicht um das Thema Disaster Recovery für virtuelle Maschinen herum. Zimmer stellt auf Basis seiner mehr als zehn Jahre Praxiserfahrung Strategien für ein erfolgreiches Backup und Recovery vor. Dies umfasst natürlich auch die Auswahl eines geeigneten Tools hierfür. Welches sich für welche Einsatzzwecke eignet, schildert Zimmer anhand eines aktuellen Marktüberblicks.

Um einem aufwändigen Recovery komplett aus dem Weg zu gehen, sind Monitoring und Analyse der wichtigsten Leistungsparameter des VMware-Systems die beste Voraussetzung. Unser Dozent stellt dabei zunächst die Indikatoren vor, die ein IT-Verantwortlicher dauerhaft im Blick haben sollte, um seine Infrastruktur performant zu halten. Dabei geht er auch darauf ein, welche Unterschiede der Administrator hinsichtlich des Einsatzes von Monitoring- und Analyseprodukten kennen sollte. Auch hier schließt sich ein Marktüberblick an, der durch Zimmers eigenes, Cloud-basiertes Werkzeug abgerundet wird.

Wir würden uns sehr freuen, Sie bei unserem Training in München oder Dietzenbach begrüßen zu dürfen. Alle Informationen zu den Veranstaltungen und der Anmeldung entnehmen Sie bitte dem Kasten "VMware Best Practice".

Agenda

VMware vSphere: So läuft's rund. Praxis aus 13 Jahren.

- Strategien zum Aufbau einer vSphere-Umgebung – Netzwerk- und Storagekonfigurationen im Überblick
- Sicherheit und Sicherung
- Was läuft in den virtuellen Maschinen? Best Practices der Anwendungen
- Virtuelle Desktops betreiben
- Lieblingsfehler und Troubleshooting
- Ausblick: Management, Automatisierung, Abrechnung aus der Cloud

Wiederbelebung: Disaster Recovery für virtuelle Maschinen

- Erfolgreiche Backup-Strategien
- Produkte am Markt

Monitoring und Analyse

- vSphere-Umgebungen performant und aktiv halten
- Monitoring- versus Analyseprodukte
- Tools und Produkte am Markt
- Demo: opvizor – der tägliche Healthcheck

Ihr Referent: Dennis Zimmer

Dennis Zimmer ist Gründer und CTO der icomasoft ag und zeichnet dort verantwortlich für die technologische Ausrichtung und Weiterentwicklung des Unternehmens. Dennis Zimmer hat über die letzten Jahre viele Unternehmen bei Design, Automatisierung und Hochverfügbarkeit ihrer virtuellen Infrastrukturen beraten und diese implementiert. Zuvor arbeitete er als Senior Consultant für Konsolidierung und Storage beim Beratungsunternehmen Mightycare Solutions sowie als Virtualization Specialist bei Pillar Data Systems. Weiterhin ist er seit mehreren Jahren als Buch- und Zeitschriftenautor sowie Trainer im Virtualisierungsumfeld bekannt. Nebenberuflich betreibt er die Community-Webseite vmachine.de.

Termin & Ort

3. September 2012:
ExperTeach Trainingscenter München, Wredestrasse 11, 80335 München

10. September 2012:
ExperTeach Trainingscenter Frankfurt/Dietzenbach, Waldstrasse 94, 63128 Dietzenbach

Das Training findet von 10:00 bis 17:30 Uhr statt.

Teilnahmegebühren

Für IT-Administrator Abonnenten 145 Euro und für Nicht-Abonnenten 195 Euro (jeweils zzgl. 19% MwSt.). Die Teilnehmerzahl ist auf 25 begrenzt.

Anmeldeschluss: 24. August (München) beziehungsweise 31. August (Dietzenbach)

Training "VMware Best Practice"

Das erste echte virtuelle Rechenzentrum

Infrastructure as a Service (IaaS) der nächsten Generation!

ProfitBricks – Hosting von Experten für Experten

Achim Weiß war über zehn Jahre verantwortlich für die technische Infrastruktur der Internetdienste bekannter Marken wie 1&1, GMX und Web.de. 2010 versammelte er ein internationales Team von 50 Ingenieuren aus verschiedenen Spezialgebieten in Berlin und entwickelte mit diesem Team in 2 Jahren auf Basis modernster Cloud-Technologien die nächste Generation von Hosting: das virtuelle Rechenzentrum.

„Wir sind ein Infrastructure as a Service (IaaS) Anbieter. Bei uns können Sie ein virtuelles Rechenzentrum mieten und es ganz nach Ihrem Bedarf mit Servern, Storage, Loadbalancern und Firewalls ausstatten - genau wie in einem realen Rechenzentrum. Doch im Gegensatz zu „realer" Hardware lässt sich die eingesetzte Hardware bei uns jederzeit an Ihre Bedürfnisse anpassen. Sie bezahlen dabei nur, was Sie tatsächlich benötigen und können Ihr virtuelles Rechenzentrum auch jederzeit an Ihre aktuellen Anforderungen anpassen."

Achim Weiß
Gründer und CEO

IaaS made in Germany

MEMBER OF united internet

Mit moderner Cloud-Technologie Zeit und Geld sparen

Ihr eigenes virtuelles Rechenzentrum

Im Gegensatz zu anderen Anbietern im Markt für Infrastructure as a Service (IaaS), hat ProfitBricks die Virtualisierung von Rechenzentren zu Ende gedacht. ProfitBricks schränkt Sie beim Aufbau Ihres virtuellen Rechenzentrums in keiner Weise ein. Es gibt keine festen Server-Konfigurationen, keine Laufzeiten, keine Einschränkung bei der Netzwerk-Infrastruktur. Und alles ist einfach und übersichtlich über den einzigartigen grafischen Data Center Designer (DCD) konfigurierbar.

Grafische Benutzeroberfläche (DCD)
Mit unserem einzigartigen ProfitBricks Data Center Designer (DCD) gestalten Sie Ihr virtuelles Rechenzentrum einfach und behalten jederzeit den Überblick.

Doppelt redundante Storage
Die Speicherung Ihrer Daten erfolgt durch zwei synchron arbeitende Sub-Units, die jeweils in sich den kompletten Datenbestand noch einmal redundant halten.

Maßgeschneiderte Server
Konfigurieren Sie Prozessorleistung, RAM und Festplattenplatz genau nach Ihren Bedürfnissen und erhalten Sie so die optimale Leistung zum optimalen Preis.

Vermaschte InfiniBand-Vernetzung
Hochgeschwindigkeit und Ausfallsicherheit bietet Ihnen unsere InfiniBand-Infrastruktur. Für Ihre Server stellt sie sich als Ethernet dar, ist aber mit bis 80 GBit/s 10-100x schneller.

Freie Vernetzung
Echte Isolation Ihres Netzwerkes im virtuellen Rechenzentrum und damit volle Freiheit bei der Vernetzungsstruktur - eine der Besonderheiten bei ProfitBricks.

SysAdmin Support
Wenn Sie den ProfitBricks Support einmal benötigen, sprechen Sie mit einem erstklassig ausgebildeten Support-Ingenieur auf dem Niveau eines erfahrenen Systemadministrators.

Einfachstes Preismodell
ProfitBricks IaaS ist Highend-Leistung zu überraschend günstigen Konditionen. Das einfachste Preismodell der Branche hilft Ihnen bei der Prognose der Kosten und beim Vergleich.

1 CORE = 4 Compute Units	4 ct*/Stunde
1GB RAM	0,5 ct*/Stunde
1GB STORAGE	4 ct*/30 Tage
1GB TRAFFIC	6 ct*/GB

Server ab 5ct* / Stunde
Minutengenaue Abrechnung
Virtueller Server mit 1 Core, 1GB RAM und 90 GB Festplatte. Traffic wird zusätzlich berechnet

Kostenlos und unverbindlich testen!
http://profitbricks.com/ia

Info-Hotline: 0800-2244668

*nur für gewerbliche Nutzung (Unternehmer), zzgl. 19% MwSt.

PROFITBRICKS GARANTIE
Keine Laufzeiten
Keine Setup-Gebühr
Minutengenaue Abrechnung
Konfiguration jederzeit änderbar

PROFITBRICKS
The IaaS-Company.

Quelle: rukanoga - 123RF

Im Test: Sophos Mobile Control 2.0

Klare Regeln für unterwegs

von Thomas Bär

Da sich mobile Endgeräte wie Smartphones oder Tablets typischerweise nicht mit den Management-Strukturen der IT verwalten lassen und keine Mitglieder des Active Directory sind, bleiben sie im Netzwerk quasi unsichtbar. Sophos Mobile Control will diese Lücke schließen und ein einheitliches Management der verschiedenen Plattformen ermöglichen. Das gelingt der Software auch zum größten Teil. Wie gut Sie als Administrator mit ihr den Gerätewildwuchs bändigen, zeigt unser Test.

Sophos Mobile Control (SMC) unterstützt Google Android, Apple iOS, Blackberry und die alternde Windows Mobile-Plattform. Die aktuelle Windows Phone-Generation von Microsoft wird nicht unterstützt, ebenso wenig die verbreitete Symbian-Umgebung. Primär dürften iOS und Android von Interesse sein, da es die beiden Systeme mit dem derzeit höchsten Verbreitungsgrad sind – und zwar in der Kategorie Mobiltelefon wie auch Tablet-System, mit und ohne 3G-Funktionalität.

Unproblematische Inbetriebnahme

Neben einem Microsoft SQL Server mindestens in Version 2005 Express verlangt die Software auch nach dem Java JDK6 oder neuer. Alle notwendigen Installations-Punkte hat der Hersteller Schritt für Schritt in einem englischsprachigen PDF-Dokument auf 35 Seiten zusammengefasst. Neben der Vorbereitung muss der Administrator lediglich einige Pfadangaben vornehmen, das SQL-Passwort für den sa-Account eingeben oder die Windows-Authentifizierung wählen und die Administrator-Kennwörter für die SMC-Software definieren. Kommt ein deutschsprachiger SQL-Server zum Einsatz, so muss vor der Nutzung über das SQL Management Studio die Sprache für das Login auf "English" gestellt werden, ansonsten ist kein Betrieb möglich.

Die Eingabe der SMTP-Informationen ist erforderlich, sofern die Software Fehlermeldungen auch per E-Mail verteilen soll. Um eine Verbindung zu einem Mailserver nur dann zuzulassen, wenn eine "Compliance-Anforderung" erfüllt wird, ist der Exchange-Server beziehungsweise ein EAS (Exchange Active Sync)-kompatibler Mailserver zu benennen, auf dem ActiveSync aktiv ist. Um den SMC-Server, der über das Internet erreichbar sein muss, korrekt in Betrieb zu nehmen, bedarf es eines SSL-Zertifikats. Die Nutzung eines selbstsignierten Zertifikats ist zwar generell möglich, hat aber zur Folge, dass App-Installationen auf Android-basierte Mobilgeräte nicht einwandfrei funktionieren. In einem weiteren Installationsschritt kommt der "Customer Wizard" zum Einsatz, um einen neuen "Kunden" einzurichten und die LDAP-Verbindungsdaten festzulegen. Da zum Leistungsumfang ein Self Service gehört, über den die Benutzer ihre Mobilgeräte eigenständig hinzufügen können, ist die Verknüpfung mit einem Verzeichnisdienst überaus sinnvoll.

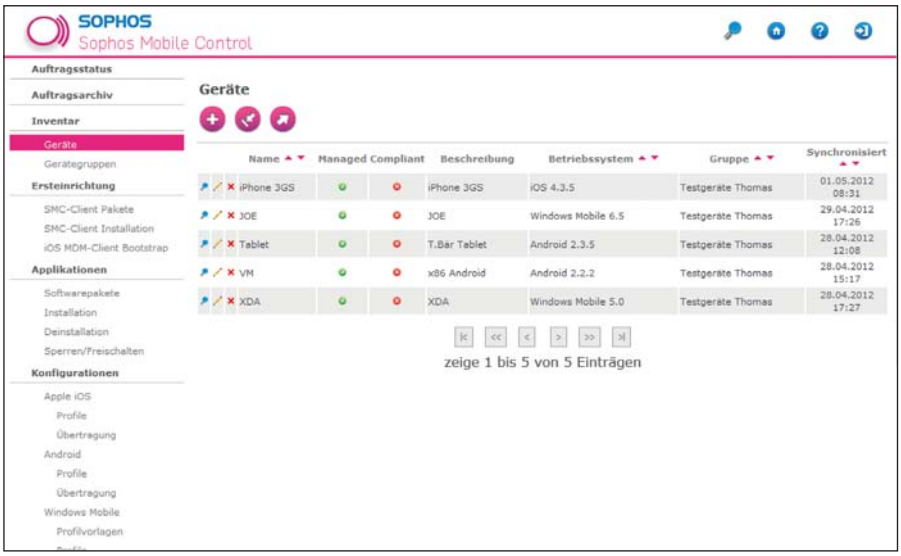


Bild 1: Mit Sophos Mobile Control können Unternehmen iOS-, Android-, BlackBerry- und Windows Mobile-Geräte zentral administrieren

Alle Plattformen unter Kontrolle

Nach der Installation erreicht der Administrator die Oberfläche über einen Webbrowser. Das Menü ist in deutscher Sprache gehalten und erklärt sich beinahe von selbst. Die Software reagierte im Test stets zeitnah. Die einzige Auffälligkeit: Ohne das passende Plug-In für Scalable Vector Graphics (SVG) erfolgt die Ansicht im Internet Explorer ohne Grafiken. Ein automatischer Log-Out-Vorgang verhindert, dass die Sitzungsfenster zu lange geöffnet bleiben. Das gleichzeitige Arbeiten von mehreren Computern in der Software verlief im Test reibungslos.

Das Menü ist in die Rubriken "Auftragsstatus", "Auftragsarchiv", "Inventar", "Ersteinrichtung", "Applikationen", "Konfigurationen", "Auftragspakete", "Backup" und "Datenzähler" unterteilt. Auf der von uns gesichteten Testplattform fanden wir bereits einige Softwarepakete, einige exemplarische Einstellungen, die als Konfiguration verschickt werden können, und die vorbereiteten SMC-Client-Installationen. Um die Suche nach Endgeräten zu vereinfachen, legten wir im Test zunächst zwei Gruppen an, in die wir die Geräte anschließend einsortierten.

Weitgehender Einfluss auf Windows Mobile

Zunächst verteilten wir für den Test den SMC-Client auf das älteste Gerät, das wir finden konnten: Ein seit Jahren ausgedientes XDA von HTC mit Windows Mobile 5.0. Im Menü "Inventar" legten wir unter "Geräte" durch einen Mausklick auf das Plus-Symbol ein neues Gerät an. Neben dem Namen mussten wir eine Beschreibung eingeben. Nach der Auswahl des Betriebssystems "Windows Mobile" ist lediglich noch die Telefonnummer des Smartphones anzugeben. Einen Mausklick später bestand die Möglichkeit, den SMC-Client auf das Gerät unter "Ersteinrichtung" zu verteilen. Im Test dauerte es nur wenige Augenblicke, bis eine SMS auf dem XDA eintraf. Über den Link in der SMS installiert der Benutzer die SMC-Software und der Client wird aktiv.

Server

Windows Server 2003 SP2 oder höher, Microsoft SQL Server 2005 Express SP2 oder höher und JDK.

Mobile Clients

Apple iOS 4.x oder höher, Android 2.2 oder höher, Windows Mobile Professional 6.1 oder 6.5, RIM BlackBerry Integration über BlackBerry Enterprise Server 5.0.3 oder höher.

Systemvoraussetzungen

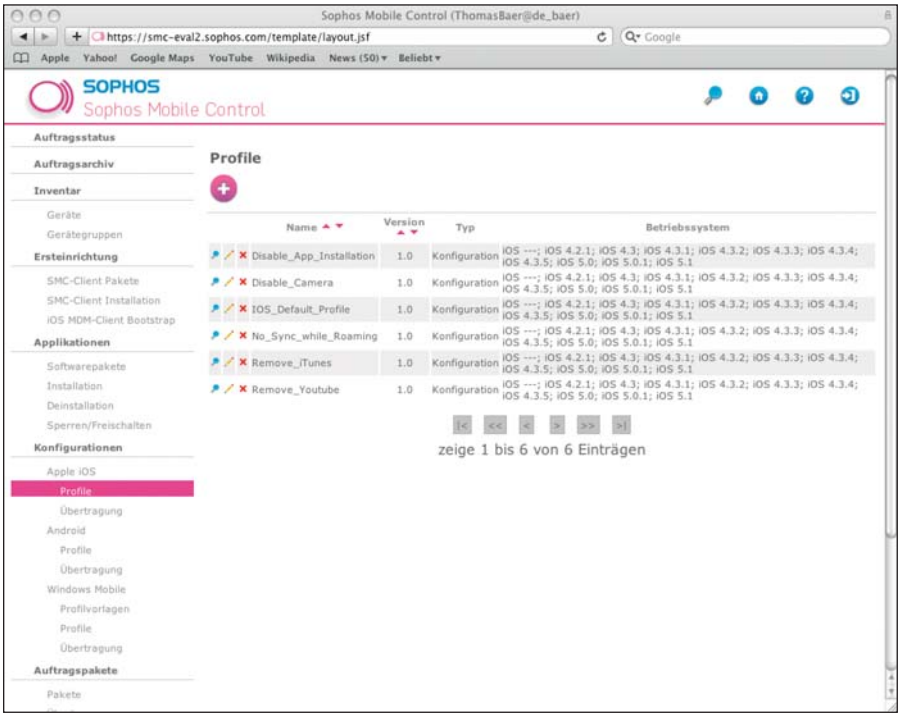


Bild 2: Mit Hilfe der Profile senden Administratoren Konfigurationspakete, hier für Apple iOS, aus. Die Pakete können zudem zu Auftragspaketen verknüpft werden.

Im Gegensatz zu den moderneren Mobilbetriebssystemen ist der Einfluss, den die SMC-Software ausüben kann, sehr groß. Das geht soweit, dass Administratoren Prozesse starten oder stoppen können und sich die Datenverbindungsdaten für Roaming, GPRS oder WLAN grafisch analysieren lassen. Wir wiederholten den Vorgang, ebenfalls ohne Schwierigkeiten, auf einem aktuellen Windows Mobile 6.5-Gerät. Die Verteilung von CAB-Dateien, die Anpassung für POP3/IMAP-Verbindungen, die Verschlüsselung des internen Speichers oder der Speicherkarte stellten kein Problem für die Software dar.

Eingeschränktes Wipe bei Android

Unsere Android-Testsysteme, eine x86-VM unter VMware Workstation und ein einfaches Tablet-System von Touchlet ohne 3G-Modul, überführten wir über den "Self Service" in das Management. Hierbei haben User die Möglichkeit, über einen einfachen Webdialog den Geräte-Typ auszuwählen und die SMC-Software per Download-Link herunterzuladen. Wie schon bei den Windows-Geräten verliefen auch hier die Tests ohne Auffälligkeiten. Bis auf eine Sache – das Ergebnis hatte es in sich: Wird der "Wipe"-Befehl, also das Kommando zum kompletten Löschen des Geräts, auf die x86-basierte VM versandt, begibt sich das Android-System in eine Endlosschleife von Neustarts. Ein bei virtuellen Maschinen nicht ganz unbekanntes Phänomen.

Freiheiten auf dem iPhone

Angesichts der großen Beliebtheit von iPhones verwundert es wenig, dass der Funktionsumfang für iOS entsprechend umfangreich ausfällt. Bedingt durch den Kommunikationsweg über den "Apple Push Notification Service" (APNS) unterscheiden sich die Funktionen kaum von den Mitbewerbern. Ab iOS in der Version 5 ist es dem Administrator möglich, die Weiterleitung von E-Mails zu verhindern, S/MIME-Einstellung einzufordern, die E-Mailfunktion für Drittanwender zu blockieren, die Autosynchronisation mit Apple iCloud zu unterbinden oder die Verwendung nicht vertrauenswürdiger Zertifikate zu blo-

Bild 3: Der integrierte "Self Service"-Webdienst ermöglicht Mitarbeitern, die persönlichen Geräte in das Management einzubinden, ohne das Smartphone aus der Hand geben zu müssen

ckieren. Eine eigene Konfigurationssoftware zur Erstellung von Profilen liefert Sophos nicht mit. Wer eigene Profile erstellen möchte, muss das kostenlose "Apple iPhone Configuration Utility" installieren, verfügbar für Max OS X und Windows, um die dort erzeugten XML-Vorlagendateien zu importieren.

Auf der iOS-Plattform können nur selbst entwickelte Apps direkt auf dem Server gehostet und von dort aus installiert werden. Die Zustimmung des Benutzers ist auch in diesem Fall erforderlich. Grundsätzlich gibt es zwei Möglichkeiten, um Apps auf Apple-Systeme zu verteilen: Aktiv über das SMC-Admin-Interface. In diesem Fall wird eine SMS mit dem Link zum Apple Appstore verschickt. Oder alternativ über den so genannten "Enterprise Appstore". Das bedeutet, dass auf dem Server die App im Admin-Interface unter Softwarepakete angelegt und mit einem Empfehlungsstatus "Erforderlich" oder "Empfohlen" versehen wird. In der SMC-App erscheinen für Benutzer diese Apps in der jeweiligen Rubrik.

Compliance überwachen

Der Dialog "Compliance-Einstellungen" dient der Konfiguration der Compliance-Prüfung. Mit ihr lässt sich feststellen, ob Geräte noch durch die Sophos-Software geprüft werden und die Unternehmensrichtlinien für den mobilen Zugriff erfüllen. Die Software steuert die Compliance-Anforderung je Mandant und je Plattform, was eine recht flexible Zuordnung erlaubt. Typischerweise setzt sich eine Compliance-Anforderung aus den folgenden Zuständen zusammen:

- Managed
- Rooting/Jailbreaking zulässig
- Passwort erforderlich
- Maximaler Zeitraum seit der letzten Synchronisation mit dem Management-Server oder
- Mindestversion des Betriebssystems

Findet die Inventarisierung unerwünschte Software, die auf einer Blacklist des Administrators aufgeführt ist, verliert ein Gerät ebenfalls den Compliance-Status. Die Möglichkeiten bei Nichteinhaltung der Compliance-Anforderungen sind jedoch technisch gering. Typischerweise bestrafen IT-Verantwortliche den Benutzer mit dem Entzug der Synchronisationsfähigkeit mit dem Mailserver. Das komplette Löschen des Geräts, der so genannte "Wipe", würde hingegen weit über das Ziel hinausschießen.

Fazit

Das Management von mobilen Geräten ist möglich – und das angesichts der Unterstützung für Windows Mobile-Systeme auch schon seit längerer Zeit. Die Software von Sophos ließ sich im Test gut bedienen und versucht die technischen Unterschiede der Plattformen zu kaschieren. Während die Lokalisierung von Android-Systemen auf einer Landkarte kein Problem darstellt, fehlt die Funktion auf Windows Mobile- oder iOS-Geräten komplett. Das Backup und Recovery von Einstellungen ist indes nur mit Android und Windows Mobile möglich. Die wichtigsten Kommandos, das Sperren und Löschen des mobilen Geräts, Inventarisierung und Verteilung von Apps, beherrscht die Software weitgehend identisch für alle Plattformen. Leider nur unter Windows Mobile verfügbar ist die Überwachung und etwaige Sperre von GSM-Verbindungen in Abhängigkeit vom Daten- oder Zeitvolumen. Auch wenn sich daher nicht alle Plattformen gleichermaßen verwalten lassen, muss der Administrator keinen Gerätewildwuchs im Unternehmen mehr fürchten. *(dr)*

Produkt
Software zur Administration von mobilen Endgeräten unter iOS, Android, Windows Mobile und Blackberry.

Hersteller
Sophos
www.sophos.de

Preis
Der Preis für 100 Geräte über eine Laufzeit von 24 Monaten beträgt rund 5.620 Euro. Enthalten sind Support, Updates, SMS für Rollout und das Abfragen von Statusinformationen.

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

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

Bedienbarkeit	7
Sicherheitsfunktionen	6
Funktionen für Android	6
Funktionen für iOS	7
Funktion für Windows Mobile	9

Dieses Produkt eignet sich

optimal für Unternehmen, die sowohl iOS, Android, Blackberry als auch noch eine sehr große Anzahl von Windows Mobile-Geräten einsetzen.

bedingt für Firmen, die nur eine sehr kleine Anzahl von mobilen Endgeräten besitzen.

nicht für Firmen, deren Mobile-Strategie auf Windows Phone oder Symbian basiert.

Sophos Mobile Control 2.0

Fähigkeiten nach Plattform				
	Apple iOS	Android	Blackberry	Windows Mobile
Self-Service: Neues Gerät anmelden	✓	✓	–	✓
Self-Service: Gerät löschen (wipe)	✓	✓	–	✓
Self-Service: Gerät lokalisieren	–	✓	–	✓
Self-Service: Gerätepasswort ändern	✓	✓	–	✓
Compliance: Management-Prüfung	✓	✓	✓	✓
Compliance: Jailbreak/Rooting Prüfung	✓	✓	–	–
Compliance: Mindestversion OS	✓	✓	✓	✓
Compliance: Blacklisting	✓	✓	✓	✓
Compliance: Maximale Synchronisationszeit	✓	✓	✓	✓
Provisioning per SMS	✓	✓	–	✓
Provisioning per E-Mail	✓	✓	–	–
Softwareinstallation ohne Benutzerinteraktion	–	–	–	✓
Softwareinstallation mit Benutzerinteraktion	✓	✓	–	✓
Inventardaten auslesen	✓	✓	✓	✓
Prozesse starten und stoppen	–	–	–	✓
WLAN blockieren	–	–	–	✓
Bluetooth blockieren	–	–	–	✓
Kamera blockieren	✓	–	–	✓
Einstellungen gegen Änderungen schützen	✓	–	–	✓
Microsoft Exchange Einstellungen setzen	✓	–	–	✓
Proxy-Einstellungen setzen	✓	–	–	✓
VPN-Einstellungen setzen	✓	–	–	✓
Festlegung von Energieoptionen	–	–	–	✓
Speicherauslastung ermitteln	✓	–	✓	✓
Ladezustand der Batterie ermitteln	✓	✓	✓	✓
Auf Roaming-Betrieb prüfen	✓	✓	✓	✓
Momentan genutztes Netz ermitteln	✓	✓	✓	✓
Kostenkontrolle durch Volumenüberwachung	–	✓	–	✓
Backup & Restore von Dateien	–	✓	–	✓
Backup & Restore von Lesezeichen	–	✓	–	✓
Backup & Restore von SMS-Nachrichten	–	✓	–	✓

Im Test: LogMeIn Hamachi 2.1

Grenzenlose Vernetzung

von Jürgen Heyer

Die zunehmende Mobilität der Mitarbeiter sowie der Bedarf nach mehr Flexibilität bei der Wahl des Arbeitsplatzes verlangen nach einer geeigneten und zugleich sicheren Lösung für eine Internet-weite Vernetzung. Statt dazu mit hohem Aufwand eigene VPN-Technik zu installieren und zu unterhalten, bietet sich als preisgünstige Alternative der Netzwerkvirtualisierungsdienst Hamachi von LogMeIn an. IT-Administrator hat sich das attraktive Angebot hinsichtlich Flexibilität und Sicherheit einmal genauer angesehen.

Die sichere Kopplung von mobilen Arbeitsplätzen untereinander oder an ein bestehendes Netzwerk ist eine anspruchsvolle Aufgabe. So sind bei einer Realisierung in Eigenregie umfassende Detailkenntnisse zur Konfiguration von VPN-Verbindungen gefragt. Auch wird geeignete VPN-Hardware benötigt oder es sind zumindest VPN-Software-Clients erforderlich. Handelt es sich bei den verwendeten Internet-Zugängen um normale DSL-Anschlüsse, besitzen diese weder feste IP-Adressen noch existiert eine nutzbare DNS-Auflösung, sodass zusätzlich ein DDNS-Dienst wie etwa dyndns.org in Anspruch genommen werden muss.

Deutlich leichter und ohne jegliche eigene Zusatzhardware gelingt eine derartige Kopplung mit dem Netzwerkvirtualisierungsdienst Hamachi von LogMeIn. Der Anbieter betreibt dazu eine eigene Internet-weite Gateway-Plattform, die in Verbindung mit sehr schlanken Clients sicher verschlüsselte Datenkanäle zwischen den jeweiligen Endpunkten aufbaut und das komplette Routing sowie den Transport der Daten übernimmt. Es handelt sich letztendlich um die gleiche Plattform, über die auch das in der Januar–Ausgabe des IT-Administrator vorgestellte LogMeIn Pro bereitgestellt wird. So konnten wir zum Test den gleichen LogMeIn-Zugang wie damals verwenden. Getestet haben wir mit der Version Hamachi 2.1.0.166.

Hamachi ist kein einmalig zu erwerbendes Produkt, sondern ein Dienst, der als Abonnement jährlich abgerechnet wird. Erfreulich ist, dass dabei eine Nutzung mit bis zu fünf Clients pro Netzwerk kostenlos ist. Damit lassen sich sehr kleine Umgebungen oder auch Testszenarien ohne finanziellen Aufwand dauerhaft betreiben.

Schneller Start mittels Registrierung

Der Einstieg in LogMeIn Hamachi ist denkbar einfach und beginnt mit einer Registrierung auf der LogMeIn-Homepage mit einer E-Mailadresse und der Festlegung eines Passworts. Abgeschlossen wird die Registrierung durch Bestätigung eines Links, den LogMeIn an die angegebene E-Mailadresse schickt. Es besteht dann gleich die Möglichkeit, den Hamachi-Client herunterzuladen und zu installieren, was dann sinnvoll ist, wenn das für die Anmeldung genutzte System zukünftig mit eingebunden werden soll. Die Installation des schlanken Clients dauert nur wenige Sekunden und erfordert keine speziellen Angaben. Neben einem Icon in der Taskleiste wird auf Wunsch eine Verknüpfung auf dem Desktop mit angelegt.

Mit der erstmaligen Anmeldung und Einrichtung eines Kontos erhält der Benutzer Zugriff auf eine Web-GUI zur Administration des Accounts mit den zugeordneten Clients und Netzwerken. Statt jedes einzubindende System für die Clientinstallation einmalig mit den Login-Daten anzumelden, kann der Administrator die gewünschten Teilnehmer in der Web-GUI über den Punkt Softwareverteilung quasi einladen. Dies ist so realisiert, dass er über einen kleinen Assistenten einen oder auch mehrere Installationslinks mit jeweils individuellen Voreinstellungen anlegt und speichert, um diese dann per Mail zu verschicken. Die Voreinstellungen umfassen die Anzahl der zulässigen Installationen, die Gültigkeitsdauer des Links (24 Stunden, eine Woche, ein Monat oder ohne Ablauf) und die Netzwerke, in die ein damit installierter Client automatisch aufgenommen werden soll. Mit Hilfe solcher Links lässt sich eine einheitliche Installation auf mehreren Systemen stark vereinfachen.

Weiterer zwingender Konfigurationsschritte auf Clientseite bedarf es nicht, auch wenn es unter einer Rubrik "Erweiterte Einstellungen" eine Vielzahl an Optionen zur Gestaltung der Benutzeroberfläche, zur Serververbindung mit dem Hamachi-Server,

Systemvoraussetzungen

Windows XP, Vista, 7, 2000, 2003 und 2008 sowie Mac OS 10.4 (Tiger), v10.5 (Leopard) oder v10.6 (Snow Leopard) auf Intel-basierten Macs, Internetverbindung.

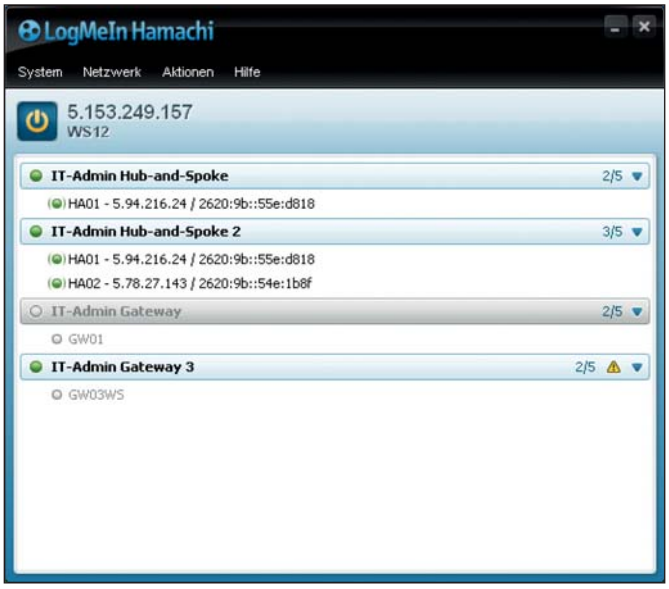


Bild 1: In der Hauptansicht des Hamachi-Clients sieht der Anwender, mit welchen Netzen er verbunden ist und welche anderen Systeme erreichbar sind

zur Peer-Verbindung, zur Chat-Einstellung, zu den Speicherorten für den Client und zur Protokollierung gibt. Die Oberfläche des Clients dient in erster Linie dazu, den Hamachi-Dienst zu starten und zu stoppen, neue Netzwerke anzulegen, bestehenden beizutreten und zu sehen, welche anderen Clients in den Netzwerken erreichbar sind. Außerdem ermöglicht eine Chatfunktion die direkte Kommunikation mit einem anderen Client. Standardmäßig wird der Client automatisch aktualisiert, sobald LogMeIn eine neue Version veröffentlicht. Diese Update-Funktion lässt sich jedoch abschalten.

Drei Netzwerktypen zur Auswahl

Um verschiedene Anforderungen an die Vernetzung zu erfüllen, kennt Hamachi drei Netzwerktypen. Gut gefallen hat uns, dass sowohl in der Web-GUI als auch im Handbuch mehrfach anschauliche Hinweise zu finden sind, welche Variante sich für welche Anforderung am besten eignet.

Alle mit allen

Der erste Typ ist das vermaschte Netzwerk, bei dem jedes Mitglied mit allen anderen Clients verbunden ist. Dieser Netzwerktyp kommt gewöhnlich zum Einsatz, wenn jedes Netzwerkmitglied erreichbar sein muss, die Kommunikation also nach Arbeitsgruppenmanier kreuz und quer erfolgen soll. Das vermaschte Netzwerk besitzt die Besonderheit, dass es der einzige Typ ist, der sich direkt vom Hamachi-Client aus anlegen lässt und somit die Web-GUI nicht zwingend benötigt. Auch ist es der einzige Typ, bei dem der Client nicht mit einem LogMeIn-Account verknüpft sein muss, sondern im sogenannten Nur-Client-Modus arbeiten kann. In diesem Fall muss ein Benutzer über seinen Client ein Netzwerk anlegen und ein Passwort vergeben, sodass sich anschließend andere Clients durch Angabe dieser Daten einklinken können. Soll ein vermaschtes Netzwerk dagegen über die Web-GUI verwaltet werden, sind die Clients zusätzlich mit einem LogMeIn-Account zu verknüpfen, LogMeIn spricht dann von einem Betrieb im Internetverwaltungsmodus.

Welcher Modus letztendlich besser geeignet ist, hängt von den Gegebenheiten ab. Ein vermaschtes Netzwerk im Nur-Client-Modus ist sicher der schnellste Weg für eine gelegentliche Nutzung. Für den produktiven Einsatz ist unserer Meinung nach der Internetverwaltungsmodus besser geeignet, da dieser gleichzeitig eine zentrale Administration erlaubt.

Recht gut konnten wir im Test beobachten, wie Hamachi die Kommunikation auf technischer Ebene realisiert: Mit der Clientinstallation wird ein zusätzlicher virtueller Netzwerkadapter namens Hamachi angelegt, der eine IP-Adresse aus dem Bereich 5.x.x.x zugewiesen bekommt. Es handelt sich hier um ein Class-A-Netz mit dem Standardgateway 5.0.0.1. Das bedeutet letztendlich, dass sich alle Internet-weit angemeldeten Hamachi-Clients im gleichen Netzsegment befinden. Die Software auf den Hamachi-Servern sorgt nun in Verbindung mit den Clients dafür, dass eine Segmentierung anhand der konfigurierten Netzwerke sowie der Accounts erfolgt, damit sich die Clients unterschiedlicher Kunden nicht gegenseitig sehen.

Eine manchmal sicher benötigte, oft aber auch unerwünschte Eigenheit des vermaschten Netzwerks ist es, dass sich die Kommunikationswege nicht strukturieren lassen, sodass letztendlich jeder Client mit jedem anderen Daten austauschen kann. Eine bessere Steuerung erlaubt die nachfolgend beschriebene Variante.

Verzahnung mit Naben und Speichen

Der zweite bei Hamachi verfügbare Netzwerktyp nennt sich Hub-and-Spoke (Nabe und Speiche). Hier fungieren ein oder mehrere Computer als Hubs, während andere Clients als Spoke konfiguriert sind. Spokes können mit den Hubs, aber nie-

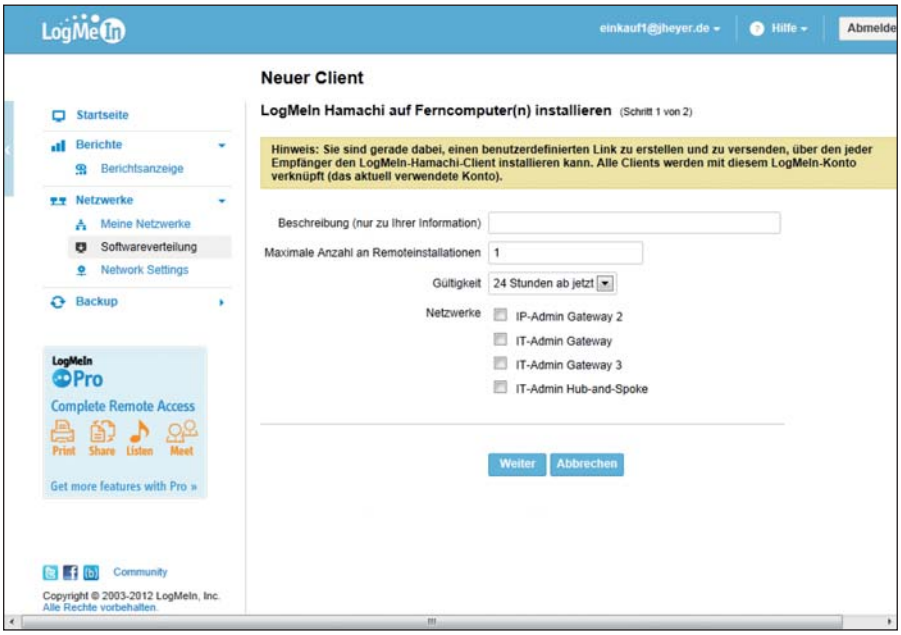


Bild 2: Bei der Erstellung eines Installationslinks lassen sich die wichtigsten Einstellungen wie Gültigkeit und Netzwerkzuordnung hinterlegen

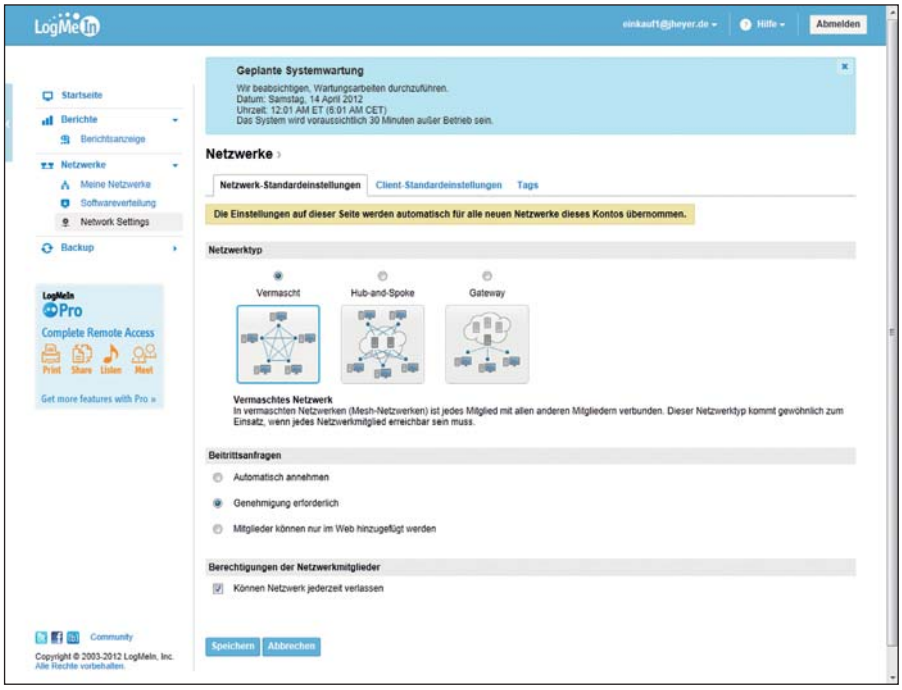


Bild 3: Um die Anlage neuer Netze zu beschleunigen, kann der Administrator in der Web-GUI individuelle Einstellungen vorgeben

mals untereinander kommunizieren, während Hubs auch gegenseitig zugreifen können. Das Hub-and-Spoke-Netzwerk kommt üblicherweise zum Einsatz, wenn einzelne Arbeitsplätze (Spokes) auf diverse Server (Hubs) zugreifen müssen. Der große Vorteil hierbei ist, dass sich die Kommunikationsbeziehungen zwischen den Netzwerkmitgliedern genauer festschreiben lassen. Zu beachten ist, dass sich quasi ein vermaschtes Netzwerk ergibt, wenn alle Teilnehmer als Hubs definiert werden. Nehmen dagegen alle als Spoke teil, so können sie untereinander nicht kommunizieren, was natürlich wenig sinnvoll ist. Ebenso wie beim vermaschten Netzwerk wird bei jedem Client ein zusätzlicher virtueller Netzwerkadapter mit einer IP-Adresse 5.x.x.x ergänzt.

Im Gegensatz zu einem vermaschten Netz muss ein Hub-and-Spoke-Netzwerk zuerst über die Web-GUI angelegt werden. Ein Client kann dann auch von sich aus beitreten, sofern in der Web-GUI zugelassen. Der Anwender muss dazu aber die eindeutige Netzwerk-ID kennen, denn der vergebene Netzname hilft nicht weiter. Im Test empfanden wir es vom Vorgehen her als deutlich übersichtlicher, die Clients anfangs nur zu installieren und den im Setup enthaltenen Punkt zum Netzwerkbeitritt zu überspringen. Nicht zugeordnete Clients erschienen dann in der Web-GUI als solche und ließen sich dort übersichtlich den Netzwerken zuweisen. Wird mit einem oben bereits erwähnten Installationslink gearbeitet, so ergibt sich die Frage nach dem Netzwerkbeitritt übrigens nicht unbedingt, da sich dies bereits bei der Link-Erstellung vordefinieren lässt.

Etwas unglücklich empfanden wir es bei einem Client-initiierten Beitritt, dass nicht gefragt wird, ob dieser als Hub oder Spoke eingerichtet werden soll, weder auf Client-Seite noch in der GUI bei der Bearbeitung der Anfrage. Per Standard wurde ein neuer Client stets als Spoke ergänzt und musste dann bei Bedarf in der Web-GUI in der entsprechenden Ansicht umkonfiguriert werden.

Bei der Arbeit mit diesem Netzwerktyp zeigte sich, dass sich die Kommunikation recht gut steuern lässt. Jeder Anwender sieht nur die Hubs und nicht alle Systeme im Netz, was die Übersicht erleichtert. Ein genereller Nachteil dieses Typs und auch des vermaschten Netzwerks ist es, dass nur Rechner mit installiertem Client teilnehmen können. Es lassen sich somit keine Netzwerkdrucker oder auch andere Geräte mit eigener IP-Adresse erreichen, wie ein NAS oder ein System mit einem nicht durch Hamachi unterstützten Betriebssystem. Um auch hierfür eine Lösung anzubieten, existiert ein weiterer Netzwerktyp.

Gemeinsame Brücke als Übergang

Der dritte Typ, das Gateway-Netzwerk, stellt letztendlich die Möglichkeit dar, ein bestehendes physikalisches Netzwerk mit Hamachi-Clients zu koppeln. Die Mitglieder eines Gateway-Netzwerks, wie beispielsweise mobile Arbeitsplätze, sehen in der Oberfläche des Hamachi-Clients einen Computer, der als Gateway für das gesamte physikalische LAN fungiert. Über dieses System können sie nun auf sämtliche Netzwerkressourcen im LAN zu-

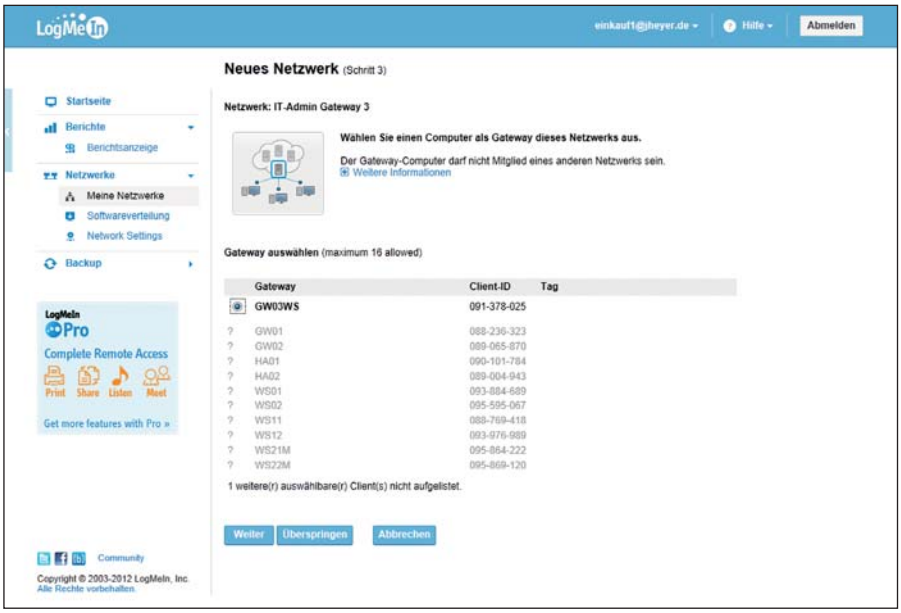


Bild 4: Beim Netzwerktyp "Gateway" lässt sich pro physikalischem Netzwerk nur ein Gateway festlegen

STRATO PRO

Born to be ROOT!

✓ keine Mindestvertragslaufzeit ✓ keine Einrichtungsgebühr

Root Server Linux Level 1. Der effiziente Sprinter!

29,00 €/Mon.*

CPU	Intel Sandy Bridge G530
Leistung	2 x 2,4 GHz
RAM	4 GB
HD	1000 GB
Traffic	Unlimited*

SICHERHEIT UND EFFIZIENZ

Sie gehen keine Kompromisse in Sachen Datensicherheit ein? Wir auch nicht! Unsere Rechenzentren sind streng nach ISO 27001 TÜV-zertifiziert. Gleichzeitig denken wir an die Umwelt und nutzen regenerative Energien.

Der Root Server Linux Level 1 von STRATO holt das Optimum an Leistung und Energieeffizienz heraus, was aktuelle Server-Hardware hergibt. Was wir an Energie sparen geben wir durch den günstigen Preis gerne an Sie weiter. Profitieren Sie davon!

* Traffic-Unlimited: Keine zusätzlichen Kosten durch Traffic (bei Traffic-Verbrauch über 1.000 GB/ Monat und danach je weitere 300 GB erfolgt eine Umstellung der Anbindung auf max. 10 MBit/s. Erneute Freischaltung der vollen Bandbreit jeweils kostenlos über den Kundenservicebereich). Alle Preise inkl. MwSt.

Info: **0 18 05 - 00 76 77** | **strato-pro.de**
(0,14€/Min. aus dem dt. Festnetz, Mobilfunk max. 0,42€/Min.)

greifen, also auch auf Netzwerkdrucker, NAS-Systeme und ähnliches. Dies ist möglich, da innerhalb des LANs der Client nur auf dem Gateway zu installieren ist, das dann als Schnittstelle dient.

In der Praxis ist das Gateway-Netzwerk am kompliziertesten einzurichten, da die meisten Einschränkungen und Randbedingungen zu beachten sind. Am besten kommt als Gateway ein Server in dem physikalischen Netzwerk zum Einsatz. Erfolgt die Clientinstallation dagegen auf einer Workstation, ist darauf zu achten, dass diese kein Mitglied einer Domäne sein darf.

Zu berücksichtigen ist weiterhin, dass nur ein System als Gateway konfiguriert werden darf und dieses auch nur Mitglied eines Hamachi-Netzwerks sein kann. Damit wird es zum SPoF (Single Point of Failure), da beim Ausfall alle Zugriffe aus dem Gateway-Netz in das physikalische unterbrochen werden. Handelt es sich bei dem Gateway um eine virtuelle Maschine, so ist zu beachten, dass die virtuellen Netzwerkadapter den Promiscuous Mode unterstützen. Bei VMware vSphere ist das standardmäßig nicht der Fall, wie wir im Test leidvoll erfahren mussten. Erst eine Suche in den Hamachi-Foren lieferte den Hinweis, warum unser Gateway gleich nach der Konfiguration die Internetverbindung verlor und sich auch nicht mehr zum Hamachi-Server verbinden konnte. Einen entsprechenden Hinweis im Handbuch suchten wir vergeblich. Nachdem wir die Einstellungen des vSwitch über unser vCenter geändert hatten, klappte die Verbindung problemlos.

Zu beachten ist ferner, dass das Gateway ohne eine zusätzliche Konfiguration nur eine Verbindung zwischen den Hamachi-Clients und den Geräten im gleichen Subnetz wie das Gateway selbst herstellen kann. Befinden sich nun, wie bei einer komplexen Netzwerkstruktur häufig der Fall, hinter dem Netz mit dem Gateway weitere (Remote)-Netze, so sind alle zu erreichenden Subnetze innerhalb der Gateway-Einstellungen zu hinterlegen, um damit letztendlich eine Routing-Tabelle aufzubauen. Gerade in komplexen Strukturen ist die Gateway-Konfiguration also nicht ganz trivial und bedarf gegebenenfalls regelmäßiger Pflege.

Die Einrichtung der Clients für ein Gateway-Netzwerk erfordert auch im Hintergrund durch Hamachi die komplexeste Netzwerkkonfiguration. Neben dem von den beiden anderen Netzwerktypen her schon bekannten virtuellen Hamachi-Adapter mit einer IP-Adresse aus dem Bereich 5.x.x.x wird noch ein weiterer Hamachi-Adapter angelegt, der eine IP-Adresse aus dem physikalischen Netz erhält. Auf dem Gateway wird zusätzlich noch eine virtuelle Netzwerkbrücke angelegt. Damit die Hamachi-Clients außerdem eine IP-Adresse aus dem physikalischen Netz bekommen, ist es erforderlich, dass es in diesem einen DHCP-Server gibt. Befindet er sich in einem anderen Subnetz als das Gateway und ist er beispielsweise aufgrund unzureichender Routing-Informationen nicht erreichbar, kann das Gateway die Aufgabe eines Quasi-DHCP-Servers übernehmen. Hierzu lässt sich der Hamachi-Client entsprechend konfigurieren.

Bild 5: Die Bearbeitung eines Netzwerks in der übersichtlichen Web-GUI erweist sich als sehr leicht

Nicht möglich ist es übrigens, mittels Hamachi zwei oder noch mehr Gateway-Netze zu koppeln. Dies erfordert dann doch spezielle VPN-Hardware. Nachdem wir im Test das anfängliche Problem mit der Promiscuous-Mode-Unterstützung gelöst hatten, konnten wir zuverlässig von den Hamachi-Clients über das Gateway auf die Komponenten im physikalischen Netz zugreifen. Auch für den Fall, dass sich mobile Clients abwechselnd im physikalischen LAN befinden sowie die Gateway-Funktion nutzen und dabei Zugriffsprobleme entstehen, hat Hamachi vorgesorgt. Für diesen Zweck lässt sich das sogenannte Heim-LAN-Verhalten konfigurieren, indem dann beispielsweise der Hamachi-Stack deaktiviert wird.

Gelungene Administration mittels Web-GUI

Recht übersichtlich fanden wir im Test die Web-GUI zum Verwalten eines Accounts. In produktiven Umgebungen sollte unserer Meinung nach die Administration in erster Linie darüber erfolgen, da sie den besten Überblick ermöglicht. Aufgelistet werden die Netzwerke mit Name, Typ und Lizenz sowie dem Nutzungsumfang. Je Netzwerk sind die enthaltenen Clients mit Verbindungsstatus, Client-ID, virtueller IP-Adresse und Client-Version aufgelistet.

In der GUI kann der Administrator Netzwerke aller drei Typen anlegen und diesen die Clients zuordnen. Weiterhin ist es möglich, für neue Netzwerke und Clients Standardeinstellungen festzulegen, um das Anlegen zu beschleunigen. Hinsichtlich der Client-Standardeinstellung kann der Administrator unterbinden, dass auf Clientseite etwas geändert wird und einige Einstellungen wie unter anderem die Verschlüsselung, die Komprimierung sowie die Chatmöglichkeit vorgeben. Auch lässt sich der Client so konfigurieren, dass dessen Benutzeroberfläche gar nicht sichtbar ist. Die eingangs bereits erwähnten erweiterten Einstellungen des Clients kann der Administrator allerdings nicht individuell vorbelegen.

Hinsichtlich der vielseitigen Konfigurierbarkeit hat Hamachi einen guten Eindruck hinterlassen. Alle Clients außer einem Gateway können durchaus Mitglied mehrerer Netzwerke sein, sodass beliebige

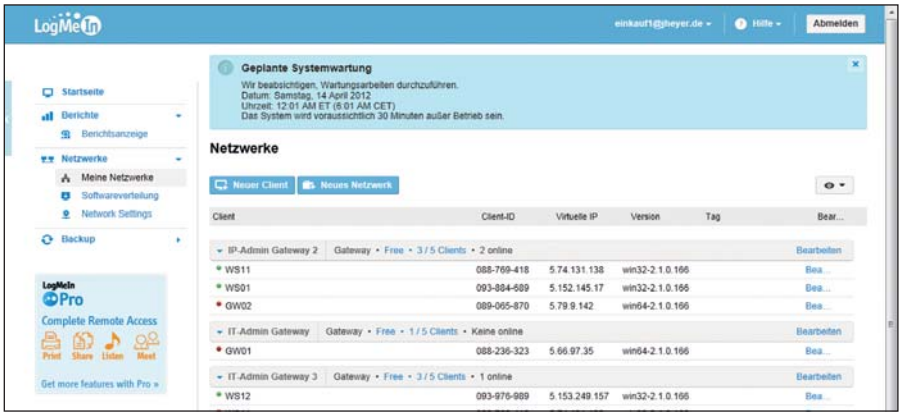


Bild 6: Die Web-GUI liefert alle zu einem Account angelegten Netzwerke und darin enthaltene Clients in einer übersichtlichen Liste

Überlappungen denkbar sind. Zu beachten ist, dass sich maximal 256 Clients in ein Netzwerk aufnehmen lassen, was aber erst in sehr großen Umgebungen zum Nadelöhr werden dürfte. Für eine einfachere Verwaltung vieler Clients hat LogMeIn mit der Hamachi-Version 2 die sogenannten "Tags" eingeführt. Dies sind Labels, also Bezeichnungen, die sich den Clients zuordnen lassen, um zusammengehörige Rechner besser zu gruppieren. Über eine Suche anhand eines Tags lassen sich diese dann einfacher finden.

Um die Beitritte zu Netzwerken zu kontrollieren, sieht Hamachi mehrere Möglichkeiten vor. So lässt sich für den Netzwerkbeitritt wie schon beschrieben ein Passwort verlangen. Bei einem durch einen Client initiierten vermaschten Netzwerk ist dies sogar obligatorisch, da es keine weitere Zugangskontrolle gibt. Bei über die Web-GUI administrierten Netzwerken kann dagegen auch eine Beitrittsgenehmigung gefordert werden. Der Administrator erhält dann eine Beitrittsanfrage, die er bestätigen muss. Auch kann er festlegen, dass neue Mitglieder nur über die GUI hinzugefügt werden dürfen. Ebenso lässt sich verhindern, dass Mitglieder ein Netzwerk von sich aus wieder verlassen. Damit lassen sich Konfigurationen sehr statisch festschreiben. Auf der Clientseite gibt es übrigens noch eine zusätzliche Sicherheitsfunktion, nämlich dass neue Netzwerkmitglieder grundsätzlich blockiert werden. In statischen Umgebungen würde dann ein Eindringling sofort abgewiesen, auch wenn es ihm beispielsweise über ein in Erfahrung gebrachtes oder erratenes Passwort gelänge, einem Netz beizutreten.

Für eine sichere Datenübertragung sind in Hamachi mehrere Mechanismen integriert. So erfolgt die Authentifizierung der Clients gegenüber den Hamachi-Servern bei LogMeIn über ein RSA-Schlüsselpaar. Daneben kommt beim Datenaustausch ein Schlüsselaustauschprotokoll (Diffie-Hellmann) zum Einsatz. Die Daten werden dann mit Hilfe einer AES-256-CBC-Chiffre blockverschlüsselt. Die Pakete werden mittels HMAC-SHA-1-96 authentifiziert und zur Vermeidung von Replay-Angriffen sind die Pakete nummeriert.

Fazit

LogMeIn Hamachi erwies sich im Test als leistungsfähiger Netzwerkvirtualisierungsdienst, der es erlaubt, Internet-weite virtuelle VPN-Netzwerke zu konfigurieren, ohne dazu eigene Hardware beschaffen zu müssen. Durch drei unterschiedliche Netzwerkarten lassen sich typische Anforderungen abdecken. So kann der Administrator mobile Benutzer untereinander vernetzen sowie mit einzelnen Servern verbinden, und es ist möglich, virtuell vernetzte Clients mit einem physikalischen LAN zu verbinden. Durch einen schlanken, sehr einfach zu installierenden Client sind die einzelnen Systeme schnell angebunden.

Gut gefallen hat uns auch die Web-GUI, mit der sich die benötigten Netzwerke übersichtlich zentral verwalten lassen. Damit ist es nicht erforderlich, dass die Anwender etwas am Client konfigurieren müssen. Eine wirksame Authentifizierung und eine leistungsstarke Verschlüsselung sorgen dafür, dass die Daten sicher im Netz transportiert werden. Interessant erscheint uns die nutzungsorientierte und zudem preislich attraktive, jährliche Abrechnung anhand der genutzten Netzwerke und Clients. Netzwerke mit bis zu fünf Clients sind sogar kostenlos, was einen einfachen und zeitlich unbegrenzten Test des Dienstes im eigenen Umfeld erlaubt. Gut kombinieren lässt sich Hamachi übrigens auch mit der Fernwartungssoftware LogMeIn Pro, wobei bei Nutzung eines gemeinsamen Accounts die gesamte Administration über dieselbe Web-Oberfläche erfolgen kann. *(ln)*

Produkt
Internet-weiter Netzwerkvirtualisierungsdienst.

Hersteller
LogMeIn
www.logmein.de

Preis
LogMeIn Hamachi kostet pro Netzwerk für bis zu 32 Clients 14 Euro jährlich. Eine Lizenz für unbegrenzt viele Netze zu je maximal 256 Clients kostet 149 Euro jährlich.

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

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

Internet-Portal	8
Clientoptionen	8
Skalierbarkeit	7
Einsatzbandbreite	9
Sicherheitsmechanismen	8

Dieses Produkt eignet sich

optimal für kleinere und mittelgroße Unternehmen, die eine überschaubare Anzahl an mobilen Clients und Heimarbeitsplätzen anbinden wollen, ohne in eigene VPN-Hardware zu investieren.

bedingt für Unternehmen, die sehr hohe Sicherheitsanforderungen an eine VPN-Anbindung haben. Hier ist zu prüfen, ob es akzeptabel ist, dass die Kommunikation, Vermittlung und Trennung der Netzwerke über Systeme erfolgt, auf die das Unternehmen keinen Einfluss hat.

nicht für Unternehmen, in denen kein Bedarf für die Anbindung externer Clients besteht oder die auf Linux setzen.

LogMeIn Hamachi 2.1

Im Test: Evalaze 1.1 Commercial Edition

Sandkastenspiele


Quelle: pixelio.de

von Jürgen Heyer

Windows-Anwendungen erfordern vor der eigentlichen Nutzung eine mehr oder minder aufwändige Installation und verankern sich dabei fest im Betriebssystem. Auch ein gelegentlich wünschenswerter Parallelbetrieb verschiedener Versionen einer Applikation ist meist nicht möglich. Abhilfe verspricht hier die Softwarevirtualisierung Evalaze, die die Anwendungen im Sandbox-Verfahren jeweils in eigene Umgebungen einpackt. Das schützt das Wirtsystem vor Veränderungen und verhindert ebenso gegenseitige Beeinflussungen. IT-Administrator hat sich den Applikations-Betrieb im Sandkasten genauer angesehen und untersucht, wie gut sich Anwendungen abschotten lassen und wie viel Aufwand der Administrator für die Paketerstellung treiben muss.

Praktisch keine Anwendung lässt bei der Installation die Registry sowie das Betriebssystem unverändert. Somit hinterlässt sie an verschiedenen Stellen Spuren und bindet sich letztendlich fest an das System. Besonders schmerzhaft zeigen sich allzu intensive Verankerungen bei Deinstallationen, wenn die Routine zum Entfernen nicht rückstandsfrei aufräumt. Im Dateisystem verbleiben dann Verzeichnisse oder einzelne Dateien und in der Registry finden sich verwaiste Einträge. Wer hat nicht schon einmal die Erfahrung gemacht, dass ein System aufgrund vieler Installationen und Deinstallationen nach und nach immer langsamer und instabiler wurde, bis letztendlich die Neuinstallation als einziger Ausweg blieb.

Um diesem Problem aus dem Weg zu gehen und die notwendigen Installationen am System zu reduzieren, stellen viele Unternehmen Applikationen mit Hilfe von Terminaldiensten zur Verfügung oder sie behelfen sich durch eine Virtualisierung ganzer PCs via VMware, Hyper-V oder anderer Produkte, um per Snapshot Systemstände einfrieren zu können. Beides erfordert aber im Hintergrund eine leistungsfähige Infrastruktur. Gerade der Weg, Programme über den Betrieb mehrerer virtueller Maschinen zu entkoppeln und sich durch Schnappschüsse die Möglichkeit offenzuhalten, ein System bei Problemen auf einen älteren Stand zurückzusetzen, schafft gleichzeitig neue Probleme. So erfordert der Betrieb mehrerer VMs entsprechende Systemressourcen und die einzelnen Systeme müssen auch gepflegt werden. Weiterhin setzt ein Snapshot stets das gesamte System zurück, statt gezielt nur auf einzelne Programme einzuwirken.

Kontrollierte Applikationen

Weitaus eleganter und zielführender arbeitet hier die Virtualisierungssoftware Evalaze der Firma Dögel aus Halle an der Saale, bei der alle Applikationen ganz normal auf dem System laufen, die Zugriffe auf das Betriebssystem aber genau kontrolliert und kanalisiert werden. Dabei haben die Programme einen ganz normalen Zugriff auf die Daten, Änderungen im Betriebssystembereich sowie in der Registry werden aber in einen dafür vorbereiteten, getrennten Speicherbereich, eine so genannte Sandbox, geschrieben, sodass eine feste Verankerung im System vermieden wird. Auch müssen die Programme vorher nicht installiert werden, sondern es ist nur eine mit Evalaze erzeugte, ausführbare Datei einzuspielen. Bei deren ersten Aufruf wird die Sandbox eingerichtet und dann die eigentliche Applikation gestartet. Um nun ein Programm wieder rückstandsfrei vom System zu entfernen, sind nur der Sandboxbereich und die ausführbare Datei zu löschen. Es gibt sogar eine Einstellung, bei der die Sandbox bei Programmende automatisch wieder entfernt wird, aber dazu kommen wir weiter unten.

Getestet haben wir Evalaze 1.1 Commercial Edition, die eine kommerzielle Nutzung und damit den Einsatz im Unternehmen erlaubt. Darüber hinaus gibt es eine Professional Edition für den privaten Gebrauch sowie eine kostenlose Free Edition, die aber funktional sehr eingeschränkt ist und neben dem Einsatz eines Assistenten keine Anpassungen erlaubt. Zum genauen Vergleich hat der Hersteller auf seiner Website (siehe Bewertungskasten

Capture-System (Builder)

Physische oder virtuelle Maschine mit Windows XP, .NET 2.0.

256 MByte Arbeitsspeicher, 15 MByte Festplattenkapazität zuzüglich mindestens der vierfache Speicherplatz der zu virtualisierenden Anwendung.

Ziel-System

System- und Hardwareanforderungen der zu virtualisierenden Anwendung, Windows XP SP2 oder höher, Windows Server 2003 oder höher.

Systemvoraussetzungen

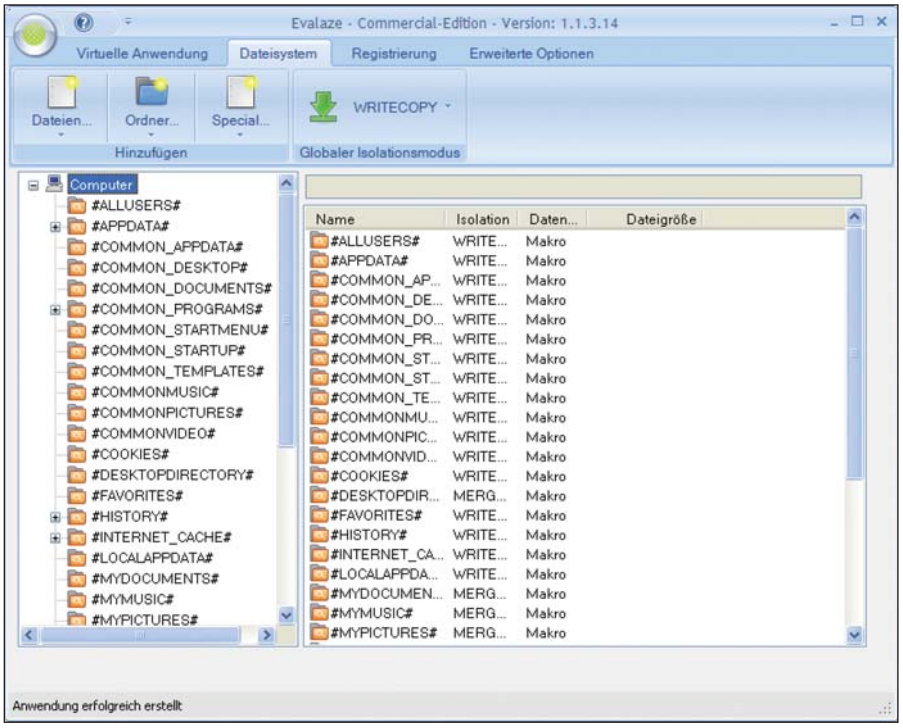


Bild 1: Beim Aufbau der Sandbox legt Evalaze eine komplexe Ordnerstruktur an, wobei sich für jedes Verzeichnis der Isolationsmodus individuell vorgeben lässt

am Ende des Artikels) den Funktionsumfang der drei Versionen in einer Übersicht nebeneinander gestellt.

Am Anfang steht der Paketbau

Der Anwender der virtualisierten Applikationen kommt mit Evalaze überhaupt nicht in Kontakt, nur der Administrator, der mit dem Tool die entsprechenden Pakete baut, die er jeweils als ausführbare Datei weitergibt. Evalaze selbst ist auf einem möglichst nackten System zu installieren, das im Idealfall nur das Betriebssystem inklusive der Patches enthält. Dies ist der so genannte Builder. Am besten nutzt der Administrator eine virtuelle Maschine, wobei der verwendete Hypervisor keine Rolle spielt. Zweck ist es, dass er so nach der Installation von Evalaze einen Snapshot ziehen und nach jeder Paketerstellung das System wieder auf diesen Stand zurücksetzen kann, um so jedes Mal mit einem definierten, sauberen Ausgangszustand zu starten.

Besser verständlich werden diese Hinweise bei der Betrachtung der Funktionsweise von Evalaze: Zu Beginn eines Laufs analysiert das Tool das komplette System, erstellt also quasi einen eigenen Schnappschuss. Dieser umfasst standardmäßig das Laufwerk C sowie die Registry. Anschließend wird der Administrator aufgefordert, die gewünschte Software zu installieren. Hat er dies getan, sollte er die Applikation mindestens einmal aufrufen und eventuelle Konfigurationsschritte durchführen, damit möglichst alle Startparameter richtig gesetzt sind, sodass die Anwendung anschließend komplett aufrufbereit ist. Danach führt Evalaze eine erneute Analyse durch, erfasst alle Änderungen im Dateisystem sowie in der Registry und schnürt daraus sowie aus einigen eigenen Virtualisierungskomponenten ein Paket in Form einer EXE-Datei. Weiterzugeben ist nun nur genau diese Datei, die sich dann beim Aufruf entpackt, die virtuelle Umgebung erzeugt und letztendlich das gewünschte Programm startet.

Wegen der beschriebenen Erfassung des Status sowie der Änderungen sollte das System möglichst ohne Zusätze installiert sein. Zum einen dauert die Statusermittlung um so länger, je mehr zu analysieren ist, zum anderen besteht die Gefahr, dass durch zusätzliche Software beispielsweise einige DLLs bereits vorhanden sind und dadurch mit der eigentlichen Applikationsinstallation nicht mehr ergänzt werden. Entsprechend werden sie bei der Differenzanalyse nicht erkannt und nicht mit

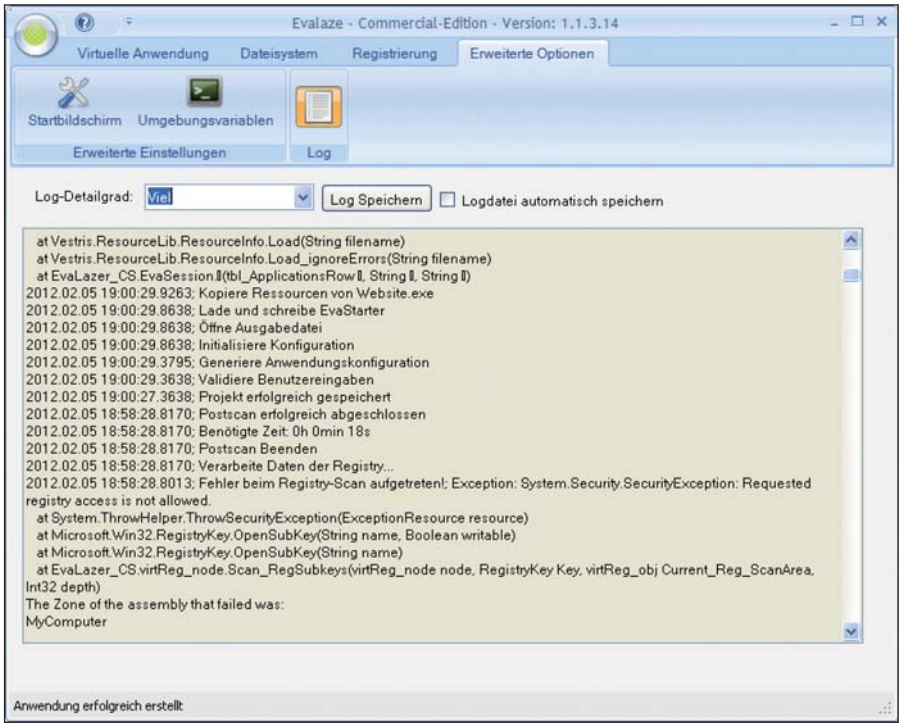


Bild 2: Sofern es beim Paketbau Probleme gibt, lohnt sich ein Blick in das detaillierte Log, um Hinweise zur Ursache zu finden

ins Paket aufgenommen. Sofern ein Zielsystem diese DLLs nicht auch bereits auf anderem Wege bekommen hat, fehlen sie letztendlich, sodass die virtualisierte Applikation nicht fehlerfrei laufen kann. So empfiehlt der Hersteller explizit, bei Nutzung von VMware als Hypervisor für den Builder nicht die VMware-Tools zu installieren, da hiermit einige DLLs im System abgelegt werden, die dann beim Capture-Vorgang womöglich nicht erfasst werden.

Der Administrator sollte auch auf einen Virenscanner verzichten und nicht benötigte Dienste, darunter speziell den Windows Update Service, deaktivieren, damit während der Paketerstellung zusätzliche Systemänderungen ausgeschlossen sind. Wichtige Updates sollten vielmehr regelmäßig manuell angestoßen werden.

Schlanke Installation

Wie schon erwähnt ist Evalaze nur auf dem Builder einzurichten, der für die Paketerstellung genutzt werden soll. Zu beachten ist, dass das .NET Framework 2.0 installiert sein muss, sonst endet das Setup sofort mit einem wenig aussagekräftigen Fehler. Auch muss die 13 MByte große Datei lokal auf den Builder kopiert werden. Ein Aufruf von einer Netzwerkfreigabe führt zu einer Fehlermeldung.

Die Installation von Evalaze ist überaus spartanisch. Beim ersten Aufruf fragt das Tool die Sprache ab und es sind der Lizenzvertrag zu bestätigen sowie der Lizenzschlüssel einzugeben – schon öffnet sich das Willkommen-Fenster, um von dort aus den Assistenten zu starten. Die Datei bleibt dabei an dem Ort, wo sie hinkopiert wurde, und muss auch von dort aufgerufen werden, da keine Menüeinträge oder Verknüpfungen auf dem Desktop angelegt werden. Letzteres kann der Administrator aber manuell durchführen, um den Aufruf zu vereinfachen.

Die Paketerstellung erfolgt entweder per Assistent oder manuell. Bei Nutzung des Assistenten werden im Gegensatz zum manuellen Ablauf einige Optionen nicht angeboten, Standardprojekte lassen sich damit aber schnell abwickeln. Im ersten Schritt sind ein Projektname und ein Zielverzeichnis anzugeben. In dem Zielverzeichnis legt Evalaze ein Unterverzeichnis mit dem Projektnamen an, den sogenannten Capture-Ordner, und speichert dort alle zum Projekt gehörigen Informationen. Weiterhin kann der Administrator hier den Scanbereich ändern, der standardmäßig das Systemlaufwerk und die Registry umfasst. Wichtig ist dabei, dass der Scanbereich auch tatsächlich alles abdeckt, was durch die spätere Installation verändert wird. Soll also beispielsweise die Installation nicht auf C, sondern auf D erfolgen, ist dieses Laufwerk entsprechend einzubeziehen. Dann wird der Prescan durchgeführt.

Anschließend fordert Evalaze zur Installation der Software auf. Hier ist darauf zu achten, dass der Administrator nicht nur

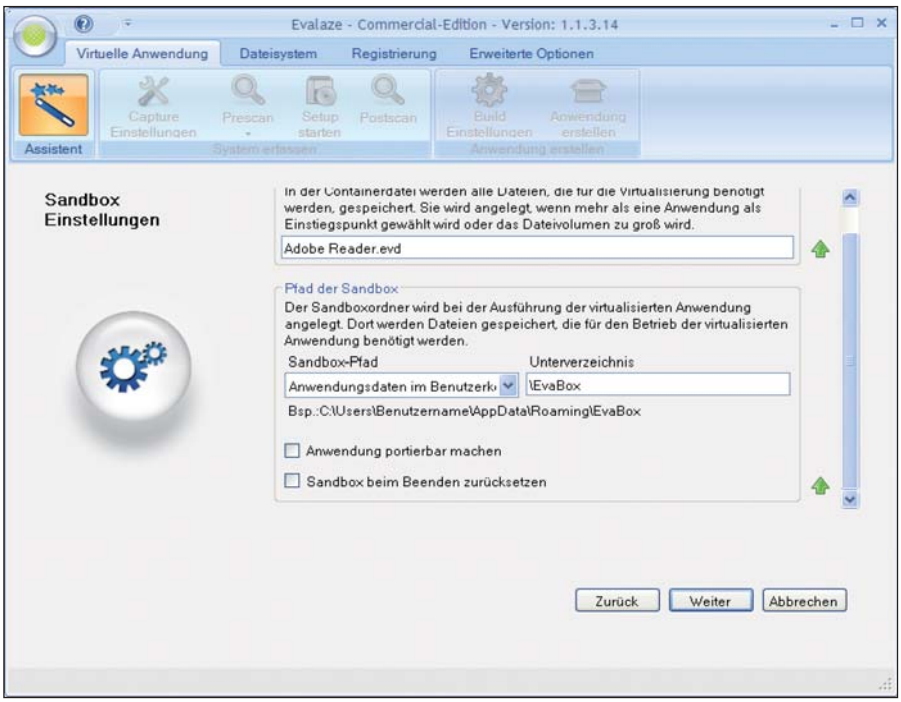


Bild 3: Der geeignete Pfad für die Sandbox richtet sich danach, wie die virtualisierte Applikation später genutzt werden soll

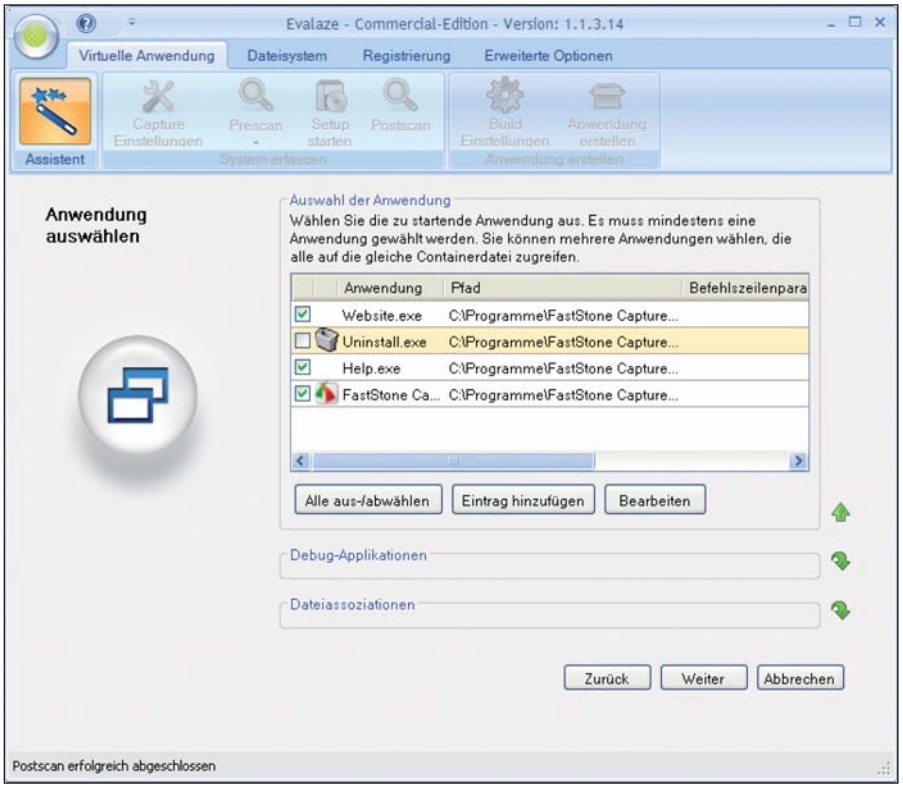


Bild 4: Evalaze versucht selbst, geeignete Einsprungpunkte für die Virtualisierung zu ermitteln und bietet dazu in Frage kommende ausführbare Dateien an

das Setup durchführen sollte, sondern auch eine eventuelle Vorkonfiguration übernimmt. Andernfalls sind dabei getätigte Basiseinstellungen nicht im Paket enthalten und die Anwender werden beim Aufruf mit entsprechenden Abfragen oder unvollständigen Vorgaben konfrontiert. Ist dies alles abgeschlossen, kann der Administrator den Postscan starten. Sofern der Scan mehrere ausführbare Dateien gefunden hat, bietet Evalaze nun diese als sogenannte Einsprungpunkte an. Sofern also eine Installation aus mehreren Programmen besteht, können diese hier ausgewählt werden. Wenig Sinn macht es verständlicherweise, Uninstall-Routinen mit auszuwählen. Fehlt ein Einsprungpunkt, so kann ihn der Administrator an dieser Stelle auch ergänzen. Ebenso lassen sich bestehende Einsprungpunkte bearbeiten, um beispielsweise einen Befehlszeilenparameter mitzugeben oder automatisch Verknüpfungen im Startmenü, auf dem Desktop oder in der Schnellstartleiste anlegen zu lassen. Standardmäßig richtet Evalaze diesbezüglich nichts ein. Auch ist es möglich, vorhandene Einsprungpunkte mehrfach mit unterschiedlichen Befehlsparametern anzulegen. Die gewünschten Verknüpfungen werden beim ersten Aufruf der virtualisierten Applikation auf dem Zielsystem eingerichtet.

Wichtig ist zu wissen, dass Evalaze nur dann eine einzelne EXE-Datei erzeugt, wenn auch nur ein Einsprungpunkt zum Aufruf gewählt wurde. Andernfalls legt das Tool für jeden Programmaufruf eine eigene, kleine EXE-Datei an und darüber hinaus eine zentrale Containerdatei, auf die alle diese ausführbaren Dateien zugreifen. Letztendlich spart das Platz, da so gemeinsame Inhalte nur einmal gespeichert werden. Bei einer Verteilung an die Anwender ist dann der komplette Dateisatz bereitzustellen, was in der Praxis aber kein Problem darstellt.

Im nächsten Schritt des Assistenten muss der Administrator den Pfad zur Sandbox festlegen und kann anschließend den Startbildschirm personalisieren. Hier lassen sich zwei Texte hinterlegen und ein eigenes Logo einbinden. Es besteht auch die Möglichkeit, gar keinen Startbildschirm einzublenden, was aber vor allem bei größeren Applikationen zur Verwirrung führen kann, da der Anwender schnell meint, es passiert nichts, während das Auspacken und Starten im Hintergrund läuft und einige Zeit dauert. Die Folge sind dann meist Mehrfachaufrufe. Abschließend ist anzugeben, wo die fertige, virtualisierte Anwendung abzulegen ist. Normalerweise ist das ein Unterverzeichnis namens "Output" in dem bereits angegebenen Projektverzeichnis. Auch das Projekt selbst lässt sich speichern, um nachträglich noch Änderungen durchführen zu können, ohne dass erneut gescannt und installiert werden muss.

Individuell definierbarer Sandkasten

Wie bereits eingangs erwähnt, besteht der Trick bei der Anwendungsvirtualisierung

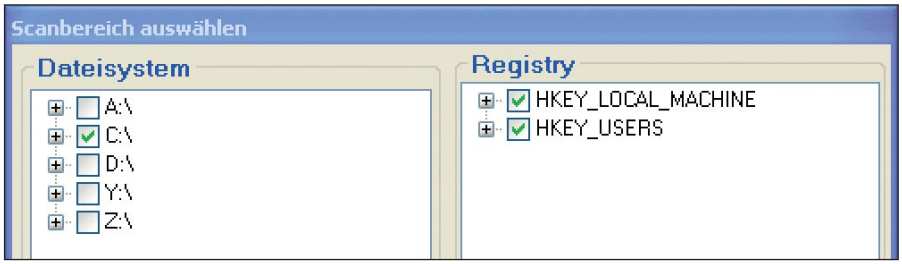


Bild 5: In der Standardeinstellung überwacht Evalaze beim Scan das Betriebssystemlaufwerk und die relevanten Teile der Registry

darin, dass alle Inhalte, die eine Anwendung eigentlich in das Betriebssystem schreibt, in einen abgeschotteten Bereich, eine Sandbox, umgeleitet werden. Wo die dazu notwendige Verzeichnisstruktur am besten angelegt wird, richtet sich nach dem Einsatzzweck eines Pakets.

Die erste Option legt die Anwendungsdaten im Benutzerkonto des Anwenders ab. Sofern mehrere Benutzer das System nutzen, wird für jeden somit eine eigene Sandbox angelegt. Das hat den Vorteil, dass auch für jeden Anwender individuelle Einstellungen gespeichert werden. Wenn es darum geht, eine Anwendung portierbar zu machen, um sie beispielsweise von einem USB-Stick aus ausführen zu können, lässt sich die Sandbox im selben Pfad wie die Anwendung einrichten. Hierfür gibt es in der Oberfläche von Evalaze auch ein Kästchen zum Anhaken, was letztendlich das Gleiche bewirkt. Weitere Optionen sind die Anlage in einem Temp-Verzeichnis oder in einem absoluten Pfad.

Normalerweise wird die Verzeichnisstruktur der Sandbox beim ersten Aufruf angelegt und bleibt dann bestehen. Dadurch dauert es beim ersten Aufruf länger, bis sich das Programm öffnet, als im Vergleich zu nachfolgenden Starts. Sofern ein Benutzer während der Programmnutzung weitere Einstellungen vornimmt, die in der Sandbox hinterlegt werden, bleiben diese erhalten. Optional gibt es auch die Möglichkeit, die Sandbox beim Beenden der Applikation zurückzusetzen. Dann wird sie jedes Mal komplett gelöscht, wodurch ein erneuter Programmaufruf natürlich etwas länger dauert. Das hat auch zur Folge, dass jedes Mal alle Einstellungen zurückgesetzt werden und die Applikation immer wieder genau so startet, wie sie bei der Paketerstellung konfiguriert wurde.

Hinsichtlich der Abschottung der Applikation vom Wirtssystem kennt Evalaze drei Stufen, hier Isolationsmodi genannt. Dies lässt sich sowohl für jeden Ordner und jede Datei der überwachten Verzeichnisstruktur als auch für die Registry einstellen. Bei "Merged" hat die Applikation den vollen Zugriff auf den Wirt und alle Änderungen werden direkt zurückgeschrieben. Dies ist beispielsweise für die benutzerspezifischen Ordner wie die eigenen Dokumente sinnvoll, damit ein Anwender dort etwas dauerhaft speichern kann.

Bei "Writecopy" versucht die Applikation, zuerst aus der Sandbox zu lesen und anschließend von der Originalstelle im Betriebssystem. Sollen eine Datei oder ein Schlüssel geändert werden, wird das Objekt vorher vom Original in die Sandbox kopiert. So bleibt das Wirtsystem unverändert. Gleiches gilt auch bei der Neuanlage von Objekten in entsprechend markierten Bereichen. Im Modus "Full" letztendlich verbirgt Evalaze die Objekte des Wirts komplett vor der Applikation, hier ist auch ein Lesen vom Original nicht möglich, sondern es besteht nur ein Zugriff auf den Inhalt der Sandbox. Diese Einstellung ist dann sinnvoll, wenn unterschiedliche Versionen einer Software parallel betrieben werden sollen.

Bereits sehr in die Tiefe geht die Möglichkeit, das Dateisystem sowie die Registry der Sandbox individuell zu bearbeiten. Der Administrator kann darin virtuelle (leere) Dateien oder Ordner sowie reale Dateien, Dateipfade, reale Ordner und Ordnerpfade anlegen. Ebenso kann er die Registry um virtuelle oder reale Werte und Schlüssel ergänzen. Auch ist es möglich, virtuelle Umgebungsvariablen zu setzen. Letztendlich sorgt dies für immense Möglichkeiten zur Anpassung. Wer sich aber dieser Mittel bedienen will, benötigt umfassende Kenntnisse hinsichtlich des Verhaltens einer Applikation und der Umsetzung in Evalaze.

Übersichtlicher Paketbau

Sind dem Administrator erst einmal die einzelnen Bedienschritte und Optionen geläufig, so sollte die Paketerstellung kein Problem sein. So begannen wir mit kleineren Paketen und dem Assistenten, was reibungslos klappte. Dann erstellten wir als etwas anspruchsvollere Aufgabe ein Paket des Adobe Reader. Obwohl hier bei der Installation zuerst nur eine kleine Setupdatei heruntergeladen wird, die dann weiteren Code aus dem Internet nachzieht, klappte auch dies problemlos. Wichtig war nur, den Adobe Reader nach der Installation zumindest einmal zu starten, damit nicht alle Anwender später den Willkommensbildschirm erhielten. Zuletzt machten wir uns an die Virtualisierung von Microsoft Office 2010, was dann nicht mehr auf Anhieb funktionierte, sodass wir beim Hersteller nachfragen mussten. Prompt bekamen wir eine entsprechende Hilfestellung, mit der wir dann auch erfolgreich waren. Die ergänzend notwendigen Schritte zeigten aber, dass es in der Praxis recht komplex werden kann, eine Applikation zu virtualisieren.

Beim Bau von Paketen, die während der Installation einen Neustart verlangen, ist es wichtig, vorher den Prescan zu speichern, da diese Informationen sonst verloren gehen und dann die Differenz nicht mehr ermittelt werden kann. Evalaze unterstützt diese Speicherung manuell, es lässt sich aber auch einstellen, dass der Prescan grundsätzlich automatisch gespeichert wird. Dann besteht nicht die Gefahr, dass dies vergessen wird.

In der getesteten Version 1.1 unterstützt Evalaze noch nicht das Virtualisieren von 64 Bit-Anwendungen. Dies kommt mit der Version 2.0, die bis zur Veröffentlichung des Tests bereits verfügbar sein müsste. Laut Hersteller soll sich an der

sonstigen hier beschriebenen Funktionalität kaum etwas ändern.

Sofern ein Projekt gespeichert wurde, lässt sich daraus jederzeit ein weiteres Paket mit etwas abweichenden Einstellungen konfigurieren, beispielsweise hinsichtlich der Lokation der Sandbox. Pre- und Postscan samt Softwareinstallation sind dann nicht erneut durchzuführen. Zu beachten ist allerdings, dass im Falle der eingangs empfohlenen Verwendung von Snapshots das Projekt vor dem Zurücksetzen gesichert werden sollte. Zu einem Projekt gehört dabei immer der gesamte Capture-Ordner. Mit Hilfe dieses Capture-Ordners ist es auch möglich, bereits virtualisierte Anwendungen erneut zu bauen, wenn beispielsweise eine neuere Version von Evalaze verfügbar ist.

Wer kein Interesse oder keine Zeit hat, selbst Pakete zu bauen, oder wer Probleme mit einer Erstellung hat, kann alternativ den Virtualisierungsservice von Dögel in Anspruch nehmen. Die Preise richten sich nach der Komplexität der zu virtualisierenden Anwendung. Prinzipiell ist es auch möglich, nur den Virtualisierungsservice zu nutzen und Evalaze selbst gar nicht zu beschaffen. Auch wenn Evalaze in der Regel nur auf einem beziehungsweise wenigen Buildsystemen installiert wird, so orientiert sich die Lizenzierung an der Anzahl der Systeme, auf denen die erstellten Pakete dann genutzt werden. Hinsichtlich der Menge der genutzten Pakete pro Client macht der Hersteller keine Lizenzvorgaben.

Fazit

Statt ganze Arbeitsplätze und Server zu virtualisieren, beschränkt sich Evalaze auf einzelne Applikationen. Realisiert wird dies, indem die Programme in einer Sandbox laufen, damit sie sich nicht fest im System verankern können. Die Sandbox virtualisiert dabei Teile des Dateisystems sowie die Registry, sodass der Datenaustausch mit dem Wirtsystem genau kontrolliert erfolgt. Ein großer Vorteil besteht darin, dass sich derart virtualisierte Applikationen sehr einfach wieder rückstandsfrei entfernen lassen und es auch möglich ist, bei Bedarf unterschiedliche Versionen einer Software parallel auf einem Betriebssystem zu betreiben, ohne dass diese sich gegenseitig stören.

Im Test klappte die Virtualisierung sowohl mit Hilfe des Assistenten als auch manuell erfreulich gut. Das Verarbeiten komplexer Applikationen wie Office erfordert aber etwas Erfahrung und gegebenenfalls eine Hilfestellung durch den Hersteller. Es gibt auch Überlegungen, für einen übergreifenden Erfahrungsaustausch ein Wiki oder ein Forum aufzubauen. Mit der getesteten Version konnten wir noch keine 64Bit-Applikationen virtualisieren, was aber mit der Version 2.0 kommt. *(jp)*

Produkt
Programm zur Anwendungsvirtualisierung.

Hersteller
Dögel
www.evalaze.de

Preis
Das Evalaze Commercial Edition Starter Pack inklusive 30 Client-Lizenzen und einer Terminal-Server-Lizenz kostet 2.142 Euro.

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

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

Paketerstellung	8
Virtualisierungsoptionen	8
Parallelbetrieb virtualisierter Applikationen	9
Entkopplung vom Zielsystem	8
Portabilität der Anwendungen	9

Dieses Produkt eignet sich

optimal für Arbeitsplätze, auf denen viele und häufig wechselnde Applikationen zum Einsatz kommen. Eine Anwendungsvirtualisierung sorgt dann auf Dauer für mehr Systemstabilität.

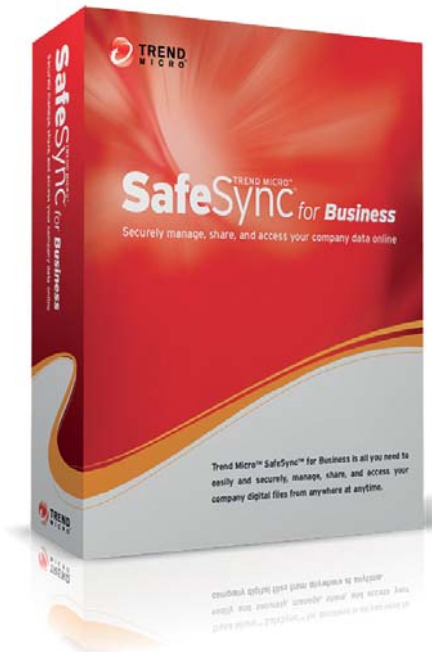
bedingt für Umgebungen, bei denen nur wenige Applikationen zum Einsatz kommen und die Konfiguration der Systeme sehr statisch ist. Hier dürfte sich der zusätzliche Aufwand nicht lohnen.

nicht für die Virtualisierung von 64 Bit-Anwendungen, diese kommt allerdings mit der Version 2.0.

Evalaze 1.1 Commercial Edition

Im Kurztest: Trend Micro SafeSync for Business

Teamwork in der Cloud



von Sandro Lucifora

Besonders für kleine und mittelständische Unternehmen ohne großes IT-Budget scheinen die vielfältigen Cloud-Angebote immer attraktiver. Doch halten längst nicht alle Produkte, was sie versprechen. Denn ein Online-Dienst muss nicht nur günstig sein, sondern auch professionellen Anforderungen genügen. SafeSync for Business von Trend Micro adressiert daher gezielt Unternehmen. Wie der Cloud-Dienst in der Praxis abschneidet, hat IT-Administrator getestet.

Während es beispielsweise in den USA bereits gängige Praxis ist, Teile des Speicherbedarfs in die Cloud zu verlagern, steht der Markt in Deutschland dieser Entwicklung noch skeptisch gegenüber. Neben dem Datenschutz- und Sicherheitsbedenken liegt das vor allem an der Tatsache, dass es noch relativ wenige deutsche Anbieter beziehungsweise deutschsprachige Angebote gibt. Trend Micro verspricht daher, die Daten seiner deutschen Kunden in einem deutschen Rechenzentrum AES-verschlüsselt abzulegen. Auch der Datentransfer findet verschlüsselt statt.

Der eigentliche Fokus von SafeSync for Business liegt dabei auf dem gemeinsamen Zugriff auf Daten mit Kollegen sowie der damit verbundenen Synchronisierung zwischen der lokalen Festplatte und dem Datenspeicher in der Wolke. Der Dienst wird nach Benutzern lizenziert und startet mit mindestens drei Usern für je 66 Euro pro Jahr. Dafür erhält der Kunde pro Zugang 50 GByte Speicherplatz, die zu einem zentralen Storage zusammengefasst werden. Dieser lässt sich in seiner Summe wiederum von allen Anwendern nutzen.

Inbetriebnahme online

Die Anmeldung für den Cloud-Dienst erfolgt – wie kaum anders zu erwarten – online. Nachdem wir unseren Zugang registriert hatten, luden wir über den Login-Bereich die aktuelle SafeSync-Software für Windows in der Version 5.0 herunter und installierten diese lokal. Die Applikation ist später für die Synchronisierung lokaler Daten mit SafeSync zuständig.

Zunächst legt SafeSync im lokalen Userverzeichnis einen SafeSync-Ordner an, in den die Daten der Online-Festplatte kopiert beziehungsweise synchronisiert werden. Im Regelfall sind lokal auch schon Ordner und Daten vorhanden, die zukünftig über SafeSync synchronisiert werden sollen. In diesem Fall haben wir über das Kontextmenü des lokalen Ordners diesen in einen SafeSync-Ordner umgewandelt. Dadurch wurden alle Dateien, die wir danach in diesem Ordner neu gespeichert, bearbeitet oder gelöscht hatten, auch im SafeSync-Ordner online aktualisiert. Somit erhielten wir in Echtzeit eine 1:1-Kopie unserer lokalen Daten.

Kleinere Probleme in der Praxis

Uns interessierte anschließend, wie sich das Produkt beim Einsatz auf Notebooks verhält. Dazu haben wir den Rechner heruntergefahren und die Internetverbindung getrennt. Danach veränderten wir die Daten über die Weboberfläche auf dem SafeSync-Laufwerk online. Nach dem Starten des Notebooks ohne Internetverbindung bearbeiteten wir ebenfalls die Daten im lokalen SafeSync-Ordner. Dann stellten wir die Internetverbindung her. SafeSync glich daraufhin die Dateien beider Orte anstandslos ab und führte sie zusammen.

Produkt
Software zur Datenhaltung und -Synchronisierung in der Cloud.

Hersteller
Trend Micro
www.trendmicro.de

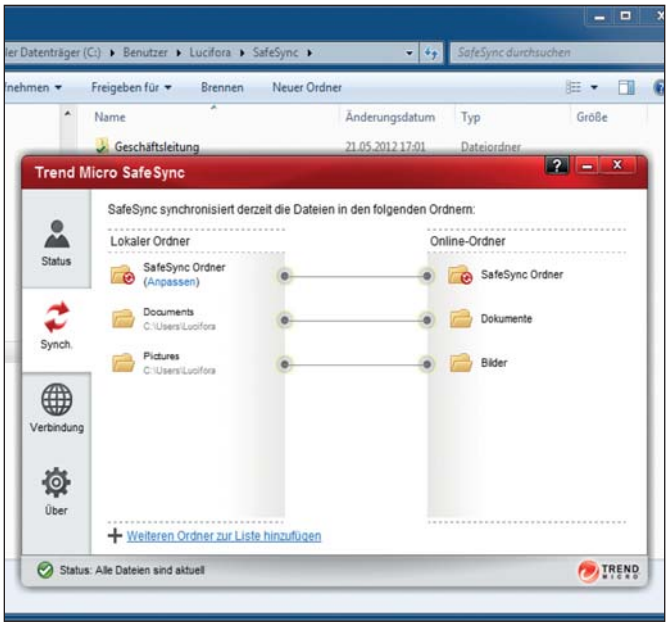
Preis
66 Euro pro Benutzer und Jahr bei drei bis fünf Benutzern.

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

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

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

Trend Micro SafeSync for Business



SafeSync hält lokale und Online-Daten synchron und spendiert pro Nutzer 50 GByte Speicherplatz

Noch einen Schritt weiter gingen wir beim Test mit dem Teamordner. Dieser ist – neben der Funktion zum Synchronisieren – das Hauptfeature von SafeSync for Business. Auf den Teamordner können mehrere Benutzer eines Unternehmens zugreifen, was das gemeinsame Arbeiten an Daten ermöglicht. Hier haben wir getestet, wie sich das Produkt verhält, wenn offline an derselben Datei gearbeitet und diese dann über SafeSync online gestellt wird. Leider machte uns SafeSync nicht darauf aufmerksam, dass es mehrfache Veränderungen einer Datei gab und verteilte immer die zuletzt synchronisierte Version an alle. Das kann natürlich ärgerlich werden – genauso wie die Tatsache, dass Dateien nicht geschützt werden, wenn sie anderweitig in Arbeit sind. Hier muss der Hersteller in jedem Fall noch nacharbeiten.

Fazit

Trend Micro zielt bei SafeSync for Business auf kleine bis mittlere Arbeitsgruppen und ermöglicht es, Daten online synchron zu halten. Auf den ersten Blick machte der Dienst einen guten Eindruck, doch zeigten sich im Laufe des Tests auch ein paar Macken. So können User nicht als Teams gruppiert werden, um Teamordner nur einer Gruppe zuzuweisen. Das Synchronisieren kann bei der gleichzeitigen Bearbeitung einer Datei oder im Offline-Modus zu Versionsverlusten führen, die sich jedoch über die Weboberfläche wieder rückgängig machen lassen. Ein Sicherheitsaspekt für Administratoren ist auch die Tatsache, dass Unternehmensdaten vielfach auf die lokalen Festplatten der Benutzer verteilt werden.

Betrachten wir nur die Synchronisierung und das damit entstehende Online- und Echtzeitbackup – also auch die Möglichkeit, dass mehrere Benutzer auf dieselben Daten zugreifen können –, zeigt sich SafeSync von seiner besten Seite. Zudem lassen sich alle Dateiformate übertragen und es besteht keine Traffic-Beschränkung. *(dr)*

Endpoint Security als Teil umfassender Sicherheitskonzepte

Trügerische Sicherheit


Quelle: L.S. - Fotolia.com

von Martin Kuppinger

Dass Endpoint Security derzeit boomt, ist keineswegs überraschend, denn in einer sich weiter verschärfenden Bedrohungslage betrachten IT-Verantwortliche mehr und mehr den Client als größtes Einfallstor für Schadsoftware. Im entsprechenden Marktsegment tummeln sich denn auch zahlreiche Anbieter mit unterschiedlichen Ansätzen und Produkten für die Endpoint Security. Und doch sollte sich der IT-Verantwortliche bewusst sein, dass die Sicherheit an den Endpunkten nur ein Teil des großen Security-Puzzles ist. Zudem bietet die Endpoint Security laufend neue Herausforderungen, beispielsweise durch "Bring Your Own Device". Welche Ansätze die Endpunkte der Unternehmens-IT sichern und welche Puzzleteile Sicherheitsverantwortliche noch bedenken müssen, zeigt dieser Beitrag.

Im Marktsegment "Endpoint Security" finden sich Produkte mit durchaus unterschiedlichem Funktionsumfang. Während ein Teil der Anbieter primär auf Antivirus und Antimalware sowie lokale Firewalls setzt, stehen bei anderen Herstellern Funktionen wie die NAC (Network Access Control), VPN (Virtual Private Networks) oder auch die Verschlüsselung von Daten auf lokalen Geräten oder auf USB-Speichermedien im Fokus. Endpoint Security ist mit Blick auf die aktuellen Angebote im Markt eher ein Marketingbegriff als eine Produktkategorie mit feststehenden Funktionen, die in jedem Fall zu erwarten sind.

Endpoint Security: Antwort auf schwindende Netzwerkgrenzen

Letzeres ist auch nicht überraschend, denn Endpoint Security ist als Konzept aus zwei Entwicklungen heraus als – je nach Hersteller – Gegenentwurf oder Ergänzung entstanden. Die wichtigere der beiden Entwicklungen ist der Schritt weg von einer primär auf den "Perimeter" ausgerichteten IT-Sicherheit, wie sie klassisch mit Firewalls als dem zentralen Element der IT-Sicherheit zu finden war (und ist).

Der Perimeter bezeichnet dabei die Grenze der Organisation respektive ihrer IT-Infrastruktur. Dieser Perimeter trennt in der klassischen Sicht die interne IT von der Außenwelt, wobei das oftmals auch mit einer Trennung von "gut" und "böse" gleichgesetzt wurde. Der Blick auf die Geschichte der Computerkriminalität zeigt allerdings, dass Letzteres noch nie richtig war – die Bedrohung kommt keineswegs nur von außen.

Dennoch hat der klassische Ansatz der Perimeter-Sicherheit so lange durchaus Sinn gemacht, wie es diesen Perimeter gab – also eine IT, die nur an sehr wenigen Stellen mit der Außenwelt verbunden war. Solange es nur eine oder wenige Schnittstellen zum Internet gab und dazu vielleicht einige direkte Einwahlverbindungen, ließen sich an diesen zentralen Verbindungsstellen auch sinnvoll Sicherheitskomponenten wie eben Firewalls platzieren. Allerdings war immer schon klar, dass Firewalls alleine nicht ausreichen für ein akzeptables oder gar hohes Maß an IT-Sicherheit.

Mit drei großen Entwicklungen hat sich das Bild nun allerdings grundlegend verändert. Die prägenden Veränderungen in der IT heute sind Social-, Mobile- und Cloud-Computing, wobei vor allem die beiden letztgenannten unmittelbare Bedeutung für das Thema Endpoint Security haben. Mit dem – keineswegs neuen – Thema Mobile Computing sind Teile der IT-Infrastruktur aus dem geschützten Perimeter heraus gewandert. Notebooks, die eben auch außerhalb des Perimeters genutzt werden können, lassen sich nicht mehr über eine ausschließlich Perimeter-basierte Sicherheit schützen. Inzwischen gibt es noch viel mehr Arten von Devices, die von Mitarbeitern verwendet werden.

Erschwerend kommt hinzu, dass nicht nur mehr Geräte mal innerhalb und mal außerhalb des Perimeters genutzt werden, sondern dass auch die Kommunikationskanäle längst nicht mehr alle der Kontrolle des Unternehmens unterliegen. Die meisten mobilen Endgeräte können sich nicht nur mit dem internen LAN oder WLAN, sondern auch direkt mit 3G-Netzwerken verbinden. Dies auch dann, wenn sie im Unternehmen genutzt werden, also zumindest geografisch innerhalb des Perimeters sind, und unter dem Aspekt der IT-Infrastruktur faktisch auch für Zugriffe von außerhalb offen sind.

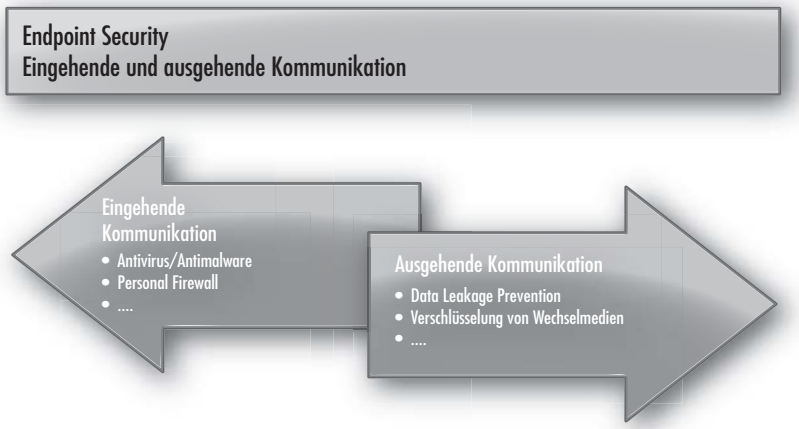


Bild 1: Endpoint Security muss mehr sein als nur lokale Antiviren-/Antimalware-Dienste und lokale Firewalls. Beide Richtungen der Kommunikation müssen unterstützt werden.

Ein weiterer Baustein des (rasenden, nicht schleichenden) Kontrollverlusts ist das Cloud Computing. Immer mehr Zugriffe berühren die interne IT-Infrastruktur nicht einmal mehr. Während die Daten beim Zugriff eines Mitarbeiters auf den im Rechenzentrum stehenden E-Mailserver oder das dort befindliche SAP-System immer noch den Weg über den (Rest des) Perimeters nehmen müssen, ergibt sich ein völlig anderes Bild, wenn als E-Maildienst beispielsweise Microsoft Office 365 verwendet wird oder SAP Business All-In-One auf der nun dafür zertifizierten AWS-Infrastruktur (Amazon Web Services) gehostet wird.

Diese "Deperimeterization", bei der es eben nicht mehr den klar definierten, kontrollierbaren Perimeter gibt, erfordert andere Lösungen für die IT-Sicherheit. Die Verlagerung der Sicherheit auf den "Endpoint", also die Endgeräte oder Endpunkte der Kommunikation, ist dabei ein Ansatz. Ob wir das als Endes des Perimeters oder als einen Ansatz, in dem jedes Gerät seinen eigenen Perimeter besitzt und diesen schützt, interpretieren, ist dabei nicht wirklich wichtig. Klar ist, dass eine klassische Perimeter-Sicherheit nicht mehr ausreicht.

Endpoints sind mehr als nur Clients

Allerdings wird bei dieser Betrachtungsweise auch deutlich, dass die Reduktion des Begriffs "Endpoint" auf "Client" oder gar "Windows-Client" nicht ausreicht. Wenn Sie ein solches Konzept verfolgen, müssen Sie alle Endpunkte schützen – also auch die Server. Allerdings haben Sie hier den Vorteil, dass Sie in klassischen IT-Infrastrukturen zumindest die im eigenen Netzwerk und Rechenzentrum betriebenen Server auch über (kleinere) Perimeter schützen können. Firewalls und andere Komponenten an der Grenze zur zentral betriebenen Server-Infrastruktur sind hier eine durchaus übliche und sinnvolle Lösung. Anders formuliert: Bei Servern, die sich in einem oder mehreren dedizierten Segmenten des Netzwerks befinden und die von den darauf zugreifenden (möglicherweise mobilen) Client-Systemen getrennt sind, braucht es nicht unbedingt eine Endpoint Security. So gesehen ist Endpoint Security in sehr vielen Infrastrukturen durchaus mit Client-Lösungen gleichzusetzen.

Klar ist aber auch: Mit Endpoint Security-Lösungen alleine werden Sie der Bedrohungen für die eigene IT nicht Herr. Es braucht das richtige und durchdachte Zusammenspiel verschiedener Lösungsansätze, um das Optimum von Aufwand und Risikoreduktion zu erreichen – und um nichts anderes geht es, denn absolute Sicherheit gibt es nicht. Auch wenn wir nur die Clients betrachten, wird in der heutigen IT-Welt deutlich, dass es bei Endpoint Security um mehr als nur Windows-Clients geht. Smartphones, Tablets, Apple iBooks und andere Systeme müssen davon ebenso erfasst werden.

Die Grenzen der Endpoint Security

Damit sind wir automatisch auch bei den Grenzen der Endpoint Security. Viele Lösungen unterstützen nicht alle der gängigen Betriebssysteme auf Endpoints. Insbesondere bei mobilen Endgeräten stoßen IT-Verantwortliche doch schnell an die Grenzen. Manchmal lassen sich diese mit Lösungen von auf solche Geräte spezialisierten Anbietern noch adressieren. Es gibt aber auch Grenzen, die sich aus der Geschlossenheit von Systemen wie dem iOS ergeben, bei dem die Eingriffsmöglichkeiten deutlich geringer als bei Windows oder Android sind.

Dies wird zunehmend zur Herausforderung, gerade mit Blick darauf, wer eigentlich heute Funktionen der Unternehmens-IT nutzen kann. Neben dem schon genannten Schlagwort "Consumerization" geht es hier auch um die "Identity Explosion", die eng damit verbunden ist. Consumerization wird typischerweise mehr mit Blick auf die Käufer von Geräten und die stärker auf den Endbenutzer ausgerichtete Funktionalität im Vergleich zur klassischen IT mit ihren Notebooks gesehen. Statt also nur einen klassischen PC in eine tragbare Form zu bringen, geht es um neue Geräte, die ganz andere Funktionen und Bedienweisen bieten, wie eben Smartphones oder die neue Generation von Tablets, die sich deutlich von den frühen Tablet-PCs unterscheiden.

Consumerization bedeutet aber auch, dass andere Personengruppen ins Spiel kommen, wenn es um die Unternehmens-IT geht. Und es bedeutet, dass andere Personengruppen die Endgeräte besitzen. Während die klassische IT ihre Sicht primär auf die Mitarbeiter fokussiert, wenn es um die Verwaltung von Benutzern und ihren Zugriffsberechtigungen geht, muss heute auch mit der oft noch überschaubaren Zahl von Endbenutzern, aber eben immer mehr auch mit anderen Gruppen wie Kunden umgegangen werden, deren Zahl oft um den Faktor 100 und mehr über der Zahl der Mitarbeiter liegt. Diese "Identity Explosion" bedeutet aber auch, dass Sicherheitsverantwortliche Schutzmechanismen überdenken müssen.

Dass Endpoint Security alleine hier nicht ausreicht wird beim Blick auf ein weiteres Schlagwort deutlich: BYOD (Bring Your Own Device). Endpoint Security-Produkte lassen sich in vielen Fällen dieses Szenarios

überhaupt nicht mehr einsetzen. Wenn das Endgerät nicht dem Unternehmen, sondern dem Mitarbeiter gehört, dann ist es rechtlich schwierig bis unmöglich, eine Installation einer bestimmten Endpoint Security-Lösung auf diesem Weg zu erreichen und dabei auch noch eine Schnittstelle zu zentralen Management- und Überwachungsfunktionen zu implementieren. Natürlich lässt sich der Zugriff auf bestimmte IT-Dienste des Unternehmens davon abhängig machen. Auch das ist aber oft nicht durchsetzbar.

Noch deutlicher wird das, wenn wir den Fall des Kunden betrachten, der auf einen Cloud-Dienst zugreift, den das Unternehmen nutzt und damit seinen Kunden anbietet. In diesem Fall gibt es weder eine direkte Berührung mit der unternehmensinternen IT-Infrastruktur noch die Möglichkeit, Endpoint Security durchzusetzen – abgesehen davon, dass sich Kunden auch bei internen Zugriffen nicht zu einem solchen Schritt bewegen lassen. Natürlich ließe sich argumentieren, dass es ja auch nicht die eigenen Geräte sind, die gefährdet sind – und im Fall der Kunden gilt auch, dass davon möglicherweise wenig Gefahr für die unternehmensinterne IT ausgeht und beispielsweise auch das Risiko von Datenlecks begrenzt ist. Das gilt aber bereits nicht mehr, wenn wir das Thema BYOD betrachten: Denn dort gibt es wenig Eingriffs- und Kontrollmöglichkeiten, aber vergleichbare Risiken für die IT-Sicherheit und von Datenlecks wie bei Endgeräten, die dem Unternehmen gehören.

Damit stellt sich die Frage, ob Sicherheitskonzepte wie beispielsweise Endpoint Security, aber auch Mobile Device Management (MDM) für mobile Endgeräte, wirklich die Lösung sein können. Die Antwort darauf ist klar: Sie können zumindest nicht die einzige Lösung sein. Und damit auch nicht die beste Lösung. Sie können aber ein Element in einer Sicherheitsstrategie sein. Wichtig ist aber, dass Sie Ihre Strategie stärker auf den Schutz von Informationen als von Geräten ausrichten. Verschlüsselungsfunktionen sind dabei ein Baustein. Sie reichen aber nicht aus. Konzepte für Enterprise/Information Rights Management (ERM/IRM) könnten wieder an Bedeutung gewinnen, insbesondere mit ihrer gewachsenen Bedeutung und verbesserten Unterstützung ab dem Microsoft Windows Server 2012. Leider gibt es aber keinen Königsweg für IT-Sicherheit: Kein einzelnes Schutzkonzept wird ausreichen. Es geht immer um die richtige und sinnvolle Kombination verschiedener Ansätze.

Endpoint Security um DLP ergänzen

Beim Blick auf Endpoint Security – die durchaus ihren Nutzen in ganzheitlichen Sicherheitskonzepten hat – wird, wie schon angesprochen, deutlich, dass es von verschiedenen Anbietern ganz unterschiedliche Lösungsansätze gibt, die unter dem gleichen Begriff verkauft werden. Das Spektrum reicht von Produkten, die sich primär auf Antivirus/Antimalware und lokale Firewall-Funktionen konzentrieren, bis zu solchen, bei denen andere Funktionen wie Gerätesperrungen, die Verschlüsselung von Wechselmedien, die Zugriffsverwaltung auf mobile Speichermedien oder auch lokale Verschlüsselungsdienste im Mittelpunkt stehen.

Die Grenzen zwischen Endpoint Security auf der einen Seite und Data Leakage Prevention (DLP) auf der anderen verlaufen fließend. Data Leakage Prevention bezeichnet Konzepte, mit denen verhindert wird, dass Daten unerlaubt und unerwünscht das Unternehmen verlassen. Das Thema gewinnt auch durch die immer strengeren rechtlichen Rahmenbedingungen an Bedeutung. Insbesondere die so genannte "breach notification", also die rechtliche Verpflichtung zur Information über Datenlecks, ist dabei ein großes Thema, weil damit massive Imageschäden, aber auch weitere rechtliche Konsequenzen verbunden sein können.

DLP ist ein Konzept, das nicht nur auf die Endgeräte beschränkt sein darf. Es spielt beispielsweise auch bei E-Mailservern eine große Rolle, wenn es darum geht zu identifizieren, welche Anhänge eben nicht an eine E-Mail angefügt werden dürfen. Andererseits gehören DLP-Funktionen auch zur Endpoint Security im weiteren Sinne, denn Sicherheit hat nicht nur etwas mit eingehender Kommunikation und hier beispielsweise dem Schutz vor Trojanern, sondern auch mit ausgehender Kommunikation zu tun.

Betrachten wir die vielschichtige Vorgehensweise bei komplexeren Angriffsszenarien, oft auch als APTs (Advanced Persistent Threats) bezeichnet, wird deutlich, wie wichtig diese Sichtweise ist. Solche Angriffe werden oft über Trojaner initiiert, die auf Clients installiert werden. Darüber werden weitere Angriffe gestartet, in deren Folge schließlich Daten an die Angreifer gesendet werden. Diese Daten lassen sich häufig aufgrund bestimmter Muster identifizieren. Wer sowohl die eingehende als auch die ausgehende Kommunikation schützt, ist grundsätzlich besser in der Lage, solche Situationen zu erkennen.

Zentrales Management und Auditing

Dies setzt dann allerdings auch voraus, dass Sie die Zusammenhänge zwischen verschiedenen Aktivitäten erkennen können. Im Hinblick auf die Endpoint Security bedeutet das, dass es eben nicht um eine isolierte Lösung geht, sondern um ein Konzept, das in übergreifende Lösungen für das Management und die Überwachung von Sicherheitsdiensten eingebunden ist.

Grundsätzlich macht Endpoint Security nur dann wirklich Sinn, wenn sich die Konfiguration auf verschiedenen Endpoints zentral steuern lässt. Endpoint Security als rein lokale Lösung kann schon deshalb nicht sicher sein, weil nicht nachvollziehbar ist, ob sie arbeitet und welche Konfigurationsänderungen ein lokaler Benutzer vielleicht vorgenommen hat, die Angriffe ermöglichen. Ein Beispiel dafür ist die Freigabe zusätzlicher Ports und Protokolle bei lokalen Firewalls, die dem Endbenutzer die Nutzung von ihm wichtigen Internet-Diensten ermöglichen, andererseits aber auch die exponierte Angriffsfläche des Systems erhöhen.

Neben dem zentralen Management und Lösungskonzepten, die eine lokale, unerkannte Veränderung von Parametern bei Endpoint Security-Lösungen verhindern, bedarf es aber auch eines zentralen Monitorings dessen, was auf den verschiedenen Endpoints geschieht. Dieses Monitoring sollte sich nicht auf die Endpoint Security beschränken, sondern mit anderen Sicherheitsdiensten integriert werden, um beispielsweise komplexere Angriffsszenarien

wie APTs erkennen zu können. Hier kommt das Thema SIEM (Security Information and Event Management) ins Spiel, also Werkzeuge, mit denen die Sicherheitsereignisse zentral erfasst und verarbeitet werden können. Neben den historischen Log-Daten und Analysefunktionen gehören dazu auch Realtime-Dienste, mit denen auf Ereignisse oder Ereigniskombinationen reagiert werden kann.

Endpoint Security ohne eine damit integrierte SIEM-Lösung ist allenfalls ein erster Schritt, aber sicher keine ausreichende Lösung. SIEM-Lösungen wiederum müssen so konfiguriert sein, dass sie alle kritischen Ereignisse zuverlässig erkennen und dabei möglichst alle unkritischen Ereignisse ausfiltern. Sie müssen dann wiederum so viele kritische Ereignisse wie möglich automatisch bearbeiten, um den Operatoren nur ein Minimum an Ereignissen für die manuelle Bearbeitung anzuzeigen.

Endpoint Security richtig genutzt

Endpoint Security kann zum Sicherheitsrisiko werden – und zwar genau dann, wenn Sie sich nach der Einrichtung von Produkten auf dem erreichbaren Teil der Desktop-Systeme (Stichwort BYOD) sicher fühlen. Das ist das gleiche Problem, das auch für alle anderen Punktlösungen im Bereich der Sicherheit gilt, insbesondere solche, die sich auf Geräte oder die Infrastruktur und nicht auf die Informationen und Dienste konzentrieren. Endpoint Security muss als ein Baustein in einem umfassenden, ganzheitlichen Konzept für IT-Sicherheit verstanden werden.

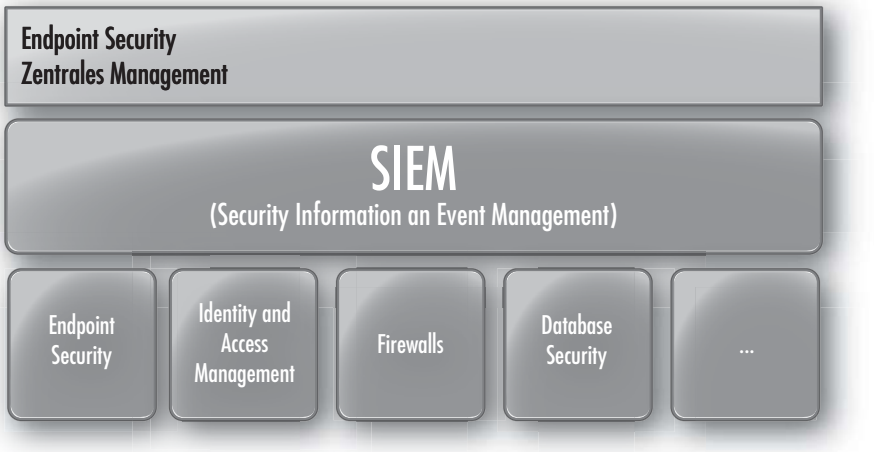


Bild 2: Zentrale Management- und Überwachungsfunktionen sind erforderlich, um Endpoint Security-Lösungen zu verwalten und die Informationen von verschiedenen Stellen – über die Endpoint Security hinaus – zu bündeln.

Der erste Schritt hin zu einem solchen Konzept ist die Risikoanalyse. Um die richtigen Maßnahmen ergreifen zu können, müssen Sie wissen, welche Bedrohungen für welche Informationen bestehen. Ein Risiko definiert sich dabei durch seine Eintrittswahrscheinlichkeit und seine Auswirkungen, also beispielsweise den Schaden für die Reputation des Unternehmens, konkrete finanzielle Schäden oder gar strategische Auswirkungen, die die Existenz des Unternehmens oder die Umsetzung von Geschäftsstrategien gefährden. Für Risiken lassen sich Gegenmaßnahmen definieren, wobei sich nicht jede Gefährdung ausschließen lässt und vor allem auf die richtige Balance von Risiko und Aufwand für die Gegenmaßnahmen zu achten ist.

Mit dem Wissen über die Risiken und einer strukturierten Analyse, die Informationen und Dienste einbezieht und damit über die systemorientierte Betrachtungsweise in der klassischen Schutzbedarfsanalyse hinausgeht, lernen Sie, wo Risiken bestehen und wie diese miteinander zusammenhängen. Es wird auch deutlich, ob und wie viel das Schließen einzelner Lücken – wie beispielsweise mit Endpoint Security – wirklich bringt. Das gerne ins Feld geführte Gegenargument bei einer solchen Vorgehensweise ist, dass der zeitliche und finanzielle Aufwand dafür hoch ist. Das stimmt, solange eine strukturierte Vorgehensweise und die dazugehörige GRC-Organisation (Governance, Risk Management, Compliance) nicht Teil der Ablauf- und Aufbauorganisation des Unternehmens sind. Wer also auf taktischer Ebene mit Endpoint Security beginnt, sollte sich trotzdem vergegenwärtigen, was er damit erreichen kann und was nicht. Darüber hinaus müssen Sie immer das Thema zentrales Management und Auditing im Blick behalten. Gerade hier wird noch einmal deutlich, dass Endpoint Security nur ein Teil einer vielschichtigen Sicherheitsinfrastruktur ist – Endpoint Security ohne SIEM ist nicht einmal die Hälfte wert.

Wichtig ist auch, dass Sie sich der Grenzen von Endpoint Security gerade mit Blick auf Themen wie BYOD bewusst sind. Sicherheitslösungen, die auf Informations- statt Gerätesicherheit abzielen, sind grundsätzlich besser geeignet, um mit diesen Herausforderungen umzugehen. Allerdings fehlt es hier oft noch an der nötigen Reife und Verbreitung von Technologien und der Unterstützung für ein komplexes, heterogenes Umfeld.

Verhaltensmuster statt Signaturen

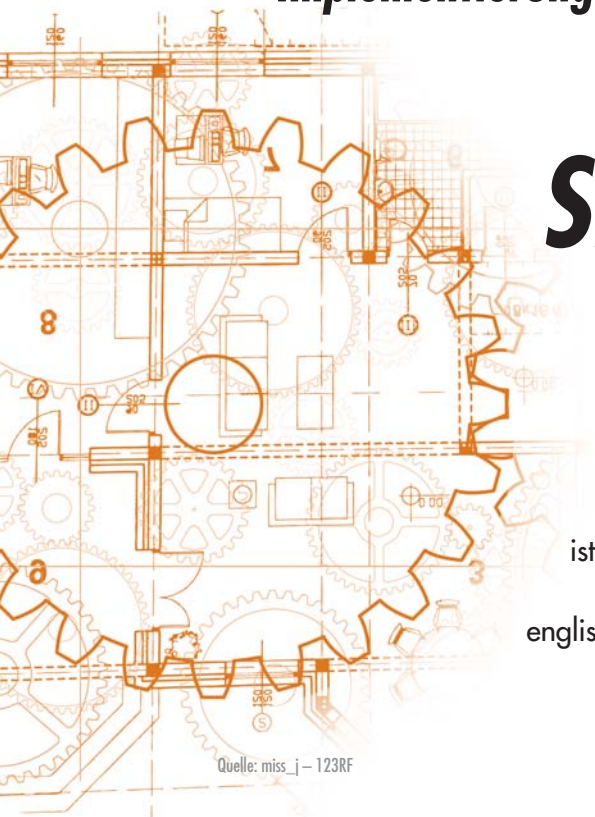
Ein auf den ersten Blick ganz anderes Thema im Zusammenhang mit Endpoint Security ist, dass sich inzwischen immer mehr die Erkenntnis durchsetzt, dass sogenannte signaturbasierte Verfahren alleine nicht ausreichen, um Viren und andere Formen von Malware zu erkennen. Denn bis zur Identifikation von Angriffen und der Verteilung von Signaturen vergeht zwangsläufig etwas Zeit – ein Zeitfenster, das von Angreifern auch genutzt wird. Das Erkennen von Verhaltensmustern von Angreifern und Angriffen ist eine weitere wichtige Funktionalität. Auch hier gilt dann aber wieder, dass solche Erkennungen von Verhaltensmustern umso besser funktionieren, je mehr Systeme betrachtet werden. Ansätze, die sich nicht nur auf ein einzelnes System, sondern auf unterschiedliche Systeme und hier wiederum nicht nur die Endgeräte konzentrieren, können grundsätzlich die besseren Ergebnisse liefern.

Fazit

Endpoint Security bringt nicht zwingend das, was Hersteller versprechen, und die Funktionsumfänge der Produkte unterscheiden sich massiv – wobei manche Anbieter solche Lösungen haben, aber eben nicht unter dem Label "Endpoint Security". Und nur bei sauber konzipiertem zentralem Management und Auditing in Verbindung auch mit anderen Sicherheitslösungen werden Sie wirklich den Mehrwert erzielen, den Endpoint Security verspricht. *(jp)*

Implementierung von System Center 2012 Endpoint Protection

Umfassende Sicherheitsarchitektur


Quelle: miss_j – 123RF

von Marc Grote

Mit System Center 2012 Endpoint Protection setzt Microsoft die konsequente Weiterentwicklung des Vorgängers Forefront Endpoint Protection 2010 fort und stattet das Produkt mit einer Vielzahl an Neuerungen und Verbesserungen aus. SCEP 2012 ist zwischenzeitlich auf dem Markt verfügbar. Dieser Artikel basiert auf zu Redaktionsschluss öffentlich zugänglichen Informationen in Form einer englischsprachigen Release Candidate-Version. Unser Workshop konzentriert sich dabei auf die wesentlichen Einstellungen und die Neuerungen. So gehen wir unter anderem auf die Konfiguration, Best Practices und das Monitoring des Sicherheitswerkzeuges ein.

Noch während einer nicht öffentlich zugänglichen Betaphase trug der Nachfolger der Forefront Endpoint Protection 2010 (FEP) den Namen Forefront Endpoint Protection 2012. Nach Abschluss dieser Betaphase entschied sich Microsoft jedoch für eine Umbenennung in System Center 2012 Endpoint Protection (SCEP) und die Integration in die System Center-Produktfamilie. Der Wechsel der Endpoint Protection aus der Familie der Forefront-Produkte zur System Center-Familie stellt sich letztendlich als logischer Schluss dar, weil die große Mehrheit der Funktionen von Endpoint Protection eine vorhandene System Center Configuration Manager (SCCM)-Umgebung voraussetzt und eine Vielzahl der administrativen Tätigkeiten mit Hilfe des System Center Configuration Manager durchgeführt werden.

Bei SCEP 2012 handelt es sich um die Enterprise Antvirus- und Antimalware-Lösung von Microsoft zum Schutz von Windows Client- und Server-Systemen. Die Verwaltung und Einrichtung der Endpoint Protection wird komplett vom System Center Configuration Manager 2012 vorgenommen. Administratoren können SCEP-Richtlinien erstellen, um das Scan-Verhalten zu steuern, und die Richtlinien basierend auf SCCM-Sammlungen den entsprechenden Servern und Clients zuweisen. SCCM 2012 stellt vielseitige Monitoring- und Reporting-Funktionen zur Verfügung, mit deren Hilfe Administratoren alle Systeme überwachen und verwalten können. Später in diesem Artikel gehen wir im Detail auf die Einrichtung und Verwaltung von SCEP ein.

Mit dem Wechsel der Forefront Endpoint Protection 2010 auf die System Center 2012 Endpoint Protection hat Microsoft auch das zugrundelegende Verwaltungssystem – System Center Configuration Manager 2007 R2/R3 auf System Center Configuration Manager 2012 – geändert und präsentiert zahlreiche Neuerungen. Zu den wesentlichen neuen Features gehören:

- Neues flaches Administrationsmodell
- Ein zentraler CAS (Central Administration Site)-Server
- Multiple Primary Flat Sites
- User Centric Management (UCM)
- Software Center
- Neue SCCM-Verwaltungskonsole
- Unterstützung für Smartphones

Installation und Administration von SCEP 2012

Die Installation setzt eine funktionierende System Center Configuration Manager 2012-Umgebung voraus. Unternehmen mit einer bestehenden SCCM 2012-Umgebung profitieren von der schnellen Implementierung von SCEP 2012. Setzen die Unternehmen noch eine ältere SCCM-2007 R2/R3 Version ein, so kann diese auf SCCM 2012 migriert werden. Ein Update-Pfad von FEP 2010 auf SCEP 2012 steht ebenfalls zur Verfügung. Dieser Artikel geht davon aus, dass eine SCCM 2012-Installation durchgeführt und die grundlegende SCCM-Konfiguration bereits vorgenommen wurde. Zu den nach der Installation durchzuführenden SCCM-Konfigurationsschritten gehören:

- Active Directory-Vorbereitungen
- Gegebenenfalls Active Directory-Schemaerweiterung
- Konfiguration des System Management Container im Active Directory
- Erstellung einer oder mehrerer SCCM Service Accounts
- SCCM-Ermittlungsmethoden konfigurieren
- SCCM-Standortgrenzen/Standortgruppen konfigurieren

- Verteilung des SCCM-Client
- Neue SCCM-Sammlungen erstellen

Nachdem Sie diese und weitere grundlegende Konfigurationsänderungen vorgenommen haben, können Sie mit der Implementierung von SCEP beginnen.

Aufspielen der Endpoint Protection-Rolle

Der erste Schritt zur Implementierung von SCEP besteht im Hinzufügen des System Center Endpoint Protection Point. Im Gegensatz zur Vorgängerversion FEP ist keine separate Installation mehr erforderlich, lediglich die SCEP-Rolle ist zum Beispiel auf einem CAS-Server zu installieren. Die Installation erfolgt mit Hilfe der SCCM-Verwaltungskonsole im Administrationsbereich: "Site Configuration / Servers and Site System Roles". Bei der Installation der SCEP-Rolle ist lediglich dem Lizenzvertrag zuzustimmen und festzulegen, ob an MAPS (Microsoft Active Protection Service) partizipiert werden soll. Bei MAPS handelt es sich um die aus der FEP 2010 bekannten Microsoft-Spynet-Mitgliedschaft, mit deren Hilfe Malware-Beispiele an den Microsoft Reputation Service übermittelt werden.

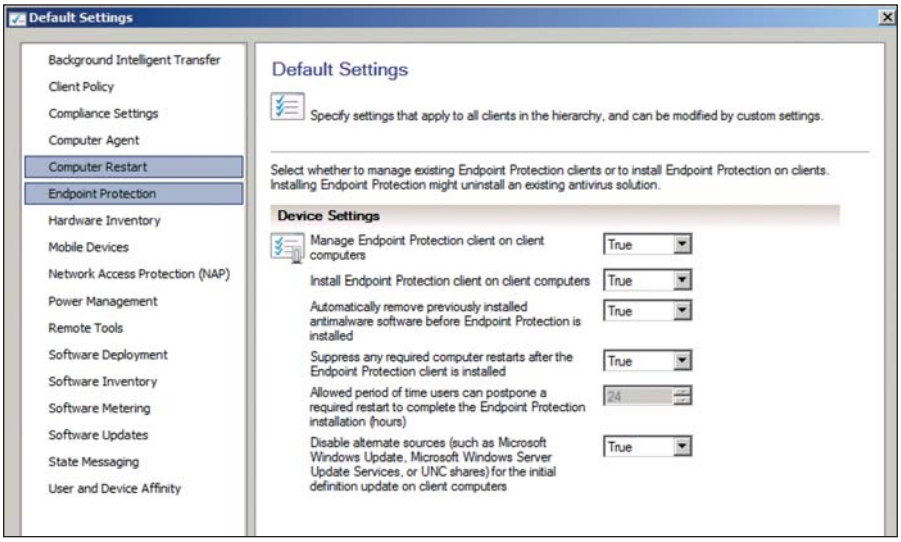


Bild 1: Aktivierung des System Center 2012 Endpoint Protection Clients

Im nächsten Schritt müssen Sie SCEP für das Client-Rollout aktivieren. Dazu können Sie die "Default Client Setting Policy" in der SCCM-Verwaltungskonsole im Administrationsbereich modifizieren, wenn geplant ist, SCEP auf allen Systemen im SCCM-Fokus zu verteilen. Für eine granularere Steuerung ist es empfehlenswert, eine neue SCCM Client-Richtlinie zu erstellen. Wenn die Default Client Setting Policy zusätzlich zu einer benutzerdefinierten Policy auf allen Systemen angewendet werden soll, wählen Sie bei der Erstellung der neuen Policy lediglich SCEP aus und legen in den Einstellungen fest, ob SCEP auf Clients und Servern installiert werden und ob eine bestehende Antivirus-Lösung eines Drittanbieters vor der Installation des SCEP-Clients deinstalliert werden soll.

SCEP 2012 ist in der Lage, einige der bekannten Antivirusprodukte von Drittanbietern automatisch im Rahmen des SCEP-Deployments zu deinstallieren, so dass Sie nicht die Deinstallationsmechanismen der Drittanbieter verwenden müssen. Hierbei ist darauf zu achten, dass etwaige Neuinstallationsmechanismen des Antivirus-Clients von Drittanbietern ausgeschaltet sind, da es sonst zu einer Schleife bei der Installation / Deinstallation des Antivirus-Clients kommen kann.

Zuweisen der SCCM Client-Richtlinie

Ein separates Installationspaket für den SCEP-Client ist in SCCM 2012 nicht mehr verfügbar. Der SCEP-Client ist Bestandteil des zu installierenden SCCM-Client, der die Kommunikation mit dem SCCM-Server ermöglicht. Der SCEP-Client wird jedoch erst nach entsprechender Aktivierung durch Zuweisung einer SCCM Client-Richtlinie zu den SCCM-Sammlungen installiert. Im nächsten Schritt ist es möglich, die neue SCCM Client-Richtlinie den im Vorfeld erstellten SCCM-Sammlungen zuzuweisen. Sobald Sie die SCCM Client-Richtlinie den SCCM-Sammlungen zugewiesen haben, beginnt SCCM 2012 mit der Installation der Endpoint Protection auf den Mitgliedern der SCCM-Sammlungen, weist hier allerdings die Default Client Malware Policy den SCCM-Sammlungen hinzu.

Bei der Default Client Malware Policy handelt es sich um die einzige Endpoint-Policy nach Hinzufügen der SCEP-Rolle und sie enthält somit nicht die notwendigen Anpassungen für den Antivirus-Scan für die einzelnen Anwendungsserver und Serverrollen, sodass es empfehlenswert ist, mit der Zuweisung der SCCM Client-

Neue Funktionen von SCEP 2012 und SCCM 2012

Die neue System Center 2012 Endpoint Protection bietet eine Reihe von Änderungen und Neuerungen gegenüber dem Vorgänger. Die umfangreichste Änderung ist die nahtlose Integration von SCEP in den System Center Configuration Manager 2012. SCEP 2012 ist jetzt eine zusätzliche SCCM-Standortserverrolle und muss nicht mehr wie FEP 2010 nachträglich zur Integration in den SCCM installiert werden. Microsoft hat SCEP mit einer Reihe von weiteren neuen und erweiterten Funktionen ausgestattet. Zu den neuen und verbesserten Funktionen gehören:

- Zentrale Verwaltung mit der SCCM 2012-Konsole
- Hohe Skalierbarkeit, angelehnt an das SCCM-Infrastrukturmodell
- Neueste Antimalware- und Rootkit-Erkennung
- Behavioral Threat-Erkennung
- Vulnerability Shielding
- Windows Firewall Management getrennt von den Endpoint Policies
- Support für System Center 2012 Configuration Manager
- Integriertes Setup, Management und Reporting
- Role Based Access Control (RBAC) basierend auf SCCM 2012
- Der SCEP-Client ist Bestandteil des SCCM-Clients
- Verschiedene SCEP-Richtlinien lassen sich zusammenführen
- Ein Client kann mehreren SCEP-Richtlinien zugeordnet werden
- Erweiterte Einstellmöglichkeiten für SCEP-Richtlinien
- Erweiterte Alarmierungs- und Protokollierungsfunktionen
- Verbesserte Antivirus-Signaturverteilung

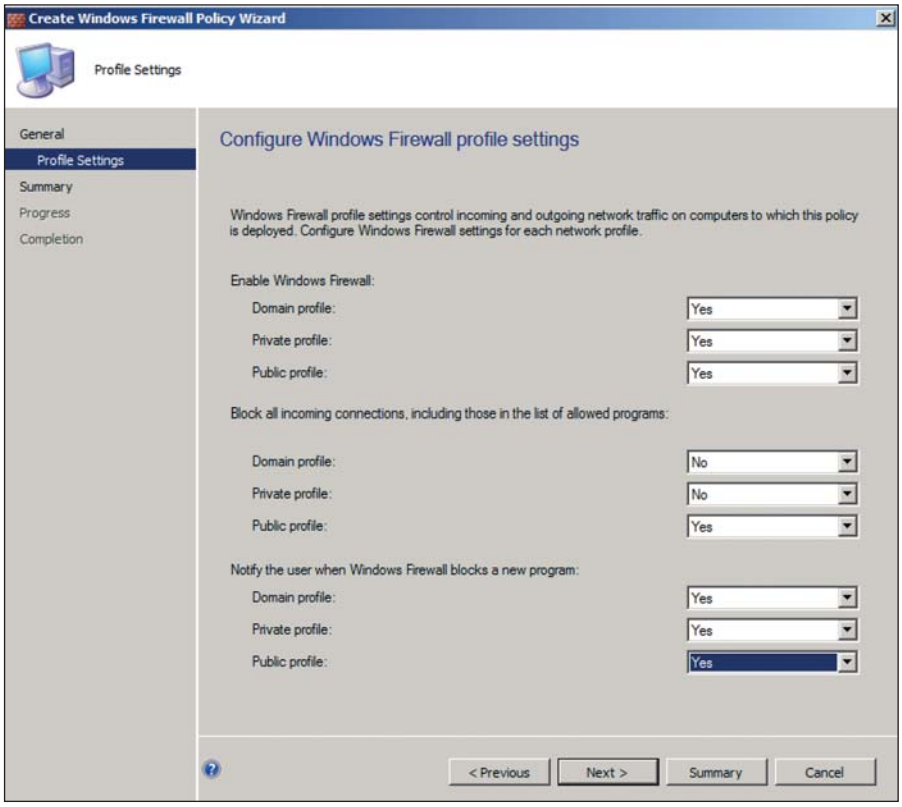


Bild 2: Steuerung der Windows Firewall durch den SCEP-Client

Richtlinie zu warten, bis Sie die entsprechenden SCEP Malware Policies erstellt haben, die die von den Softwareanbietern empfohlenen Einstellungen für den Antivirus-Scan enthalten.

Die Erstellung von angepassten Antimalware Policies erfolgt im Bereich "Assets and Compliance" der SCCM-Verwaltungskonsole. Durch das Hinzufügen der SCEP-Rolle taucht jetzt ein neuer Punkt "Endpoint Protection" in der SCCM-Verwaltungskonsole auf. Bei der Erstellung der neuen Antimalware Policy ist es möglich, folgende Einstellungen vorzunehmen:

- Scheduled Scans
- Scan Settings
- Default Action
- Real Time Protection
- Exclusion Settings
- Advanced
- Threat Overrides
- Microsoft Active Protection Service
- Definition Updates

Im Bereich "Scheduled Scans" legen Sie fest, in welchen Zeitabständen ein Quick- oder Full Scan der betroffenen Clients und Server durchgeführt werden soll und wie viel CPU-Kapazität für den Scanprozess maximal verwendet werden darf. Neu im Bereich "Scan Settings" ist die Möglichkeit, E-Mails und Anlagen zu scannen.

Malware-Policy administrieren

Im Bereich "Real Time Protection" konfigurieren Sie den Echtzeitschutz für Clients und Server. Microsoft empfiehlt, das "Behavior monitoring" und den Schutz gegen "Network based exploits" auf Serversystemen nicht zu aktivieren, da dies zu einer starken Auslastung der Systeme führen könnte. Auf Clientsystemen oder besonders zu schützenden Systemen können Sie diese Optionen jedoch in der Regel aktivieren. Im Bereich "Exlusion Settings" setzen Sie die Ausnahmen vom Scan-Prozess fest. Hierzu gehören ausgeschlossene Verzeichnisse, Prozesse und Dateitypen. Hier wird eindringlich empfohlen, die Ausnahmen basierend auf den Angaben der Software-Anbieter zu konfigurieren.

Neu im Bereich "Threat Overrides" ist die Möglichkeit, falsch erkannte Bedrohungen durch SCEP anhand einer Auswahlliste aus der Microsoft Malware-Enzyklopädie auszuschließen. Beim Vorgängerprodukt FEP war dieses ein manueller und recht aufwändiger Prozess, die Bedrohung manuell aus der Enzyklopädie zu ermitteln und in der Antimalware-Richtlinie zu hinterlegen. Gelegentlich erkennt SCEP legitim installierte Programme als Bedrohung und versucht, diese zu isolieren. Bekannte Beispiele für diese Fehlalarme sind Remoteverwaltungsprogramme wie RealVNC, Dameware und andere. Im Bereich "Definition Updates" bestimmen Sie, von wo der SCEP-Client Updates der Antimalware-Signaturen beziehen kann. Als Updatequelle stehen SCCM, Microsoft Update, WSUS, das Microsoft Malware Protection Center (MMPC) oder ein UNC-Fileshare zur Verfügung.

Nachdem Sie alle notwendigen Einstellungen in der neuen Antimalware Policy vorgenommen haben, weisen Sie diese

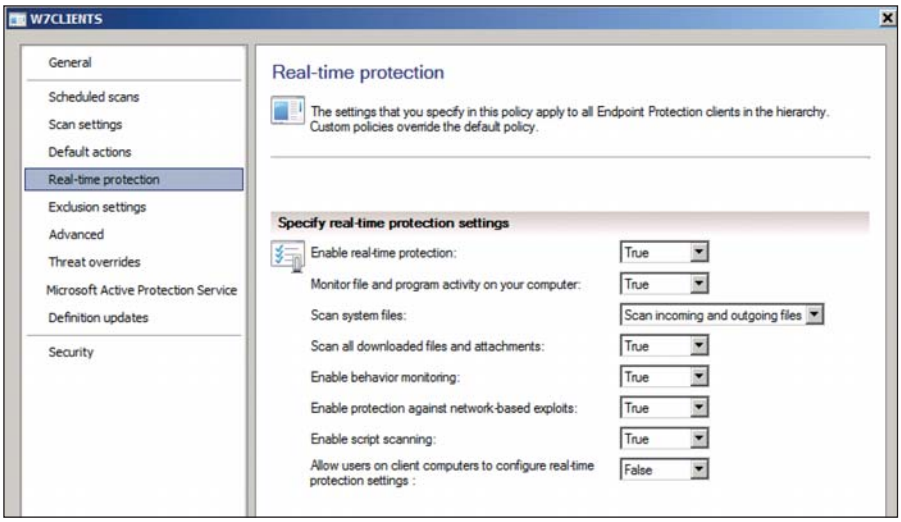


Bild 3: Die Real Time Protection sollte nur auf Clients mit allen Optionen aktiviert sein – auf Servern drohen Performance-Einbußen

Bestellen Sie jetzt

das IT-Administrator

Sonderheft I/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. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.*

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

iadministrator
Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, ich 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 0712

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

den entsprechenden SCCM-Sammlungen zu. Dazu wählen Sie im Kontextmenü der Antimalware Policy den Menüpunkt "Deploy" aus. Hier haben Sie nun die Möglichkeit, die Antimalware Policy den SCCM-Sammlungen hinzuzufügen. Neu in SCCM 2012 ist ferner die Option, mehrere Antimalware-Richtlinien zu einer neuen Richtlinie zusammenzuführen. Dies macht sehr häufig Sinn, wenn es notwendig ist, Systeme mit mehreren installierten Anwendungen oder Serverrollen zu schützen. Nachdem Sie die Antimalware-Richtlinie den SCCM-Sammlungen zugewiesen haben, weisen Sie die im Vorfeld erstellte SCCM Client-Richtlinie den SCCM-Sammlungen zu. Der SCEP-Client wird somit automatisch installiert und die entsprechende Antimalware-Richtlinie angewandt.

Mit Hilfe der SCCM-Verwaltungskonsole ist es nun auch möglich, Einstellungen für die Windows Firewall auf Endgeräten durch SCEP unabhängig von der Antimalware-Richtlinie zu steuern und den entsprechenden SCCM-Richtlinien zuzuweisen. Bei dem Vorgängerprodukt FEP 2010 war die Steuerung der Windows Firewall Bestandteil der Antimalware-Richtlinie. Bei Verwendung dieser Funktion ist darauf zu achten, dass es nicht zu Wechselwirkungen mit etwaigen Windows-Firewall-Einstellungen unter Verwendung von Active Directory-Gruppenrichtlinien kommt.

Überwachung und Monitoring

Nach der Erstellung der Antimalware-Richtlinien und der Zuweisung der SCCM Client-Richtlinie zu den SCCM-Sammlungen kann jetzt die Verteilung des SCEP-Clients mit Hilfe der SCCM-Verwaltungskonsole zentral überwacht werden und Sie können sich über den Schutz der Systeme und etwaiger Malwarefunde auf den Systemen informieren lassen und entsprechende Aktionen einleiten, um infizierte Clients und Server zu bereinigen.

In der SCCM-Verwaltungskonsole im Bereich "Monitoring" existiert ein Unterpunkt mit dem Namen "System Center 2012 Endpoint Protection Status", mit dessen Hilfe Sie die komplette SCEP 2012-Umgebung überwachen können (siehe Bild 4). Die Überwachungskonsole gibt einen Überblick über die Verteilung des SCEP-Clients, die Anzahl der mit Malware infizierten Endgeräte sowie den Status der Clients und die Aktualität der Antimalware Definitions Updates auf den Endgeräten. Durch einen Mausklick auf eine entsprechende Option in der Konsole setzen Sie den Fokus auf die SCCM-Collection mit dem Filter. Mit einem Rechtsklick auf den Client wählen Sie im Kontextmenü den Punkt "Endpoint Protection" aus und starten ein Full oder Quick Scan des Client/Servers sowie initiieren ein Update der Malware-Definitionsupdates.

Damit Sie nicht immer die SCCM-Verwaltungskonsole verwenden müssen, um sich einen Überblick über den Zustand des Malware-Schutzes von Clients und Servern zu verschaffen, stellt SCCM 2012 die Möglichkeit zur Verfügung, bei entsprechenden Malware-Vorfällen eine E-Mailbenachrichtigung an den Administrator zu senden. Um von der E-Mailbenachrichtigung Gebrauch zu machen, müssen Sie im ersten Schritt die globale SCCM E-Mailbenachrichtigung mit Hilfe der SCCM-Verwaltungskonsole aktivieren. Dies erfolgt in der SCCM-Verwaltungskonsole im Bereich "Administration / Site Configuration / Sites". Durch einen Rechtsklick mit der Maus wählen Sie im Kontextmenü des SCCM-Standorts den Punkt "Configure Site Components" aus und aktivieren dort die Benachrichtigung. Hierzu ist der Name des SMTP-Servers, der verwendete SMTP-Port, die Authentifizierung gegen den SMTP Server sowie die Absenderadresse für die E-Mailbenachrichtigungen anzugeben.

Im nächsten Schritt richten Sie in der SCCM-Verwaltungskonsole im Bereich "Monitoring / Overview / Alerts / Subscription" eine neue Benachrichtigung für Administratoren ein. Hierzu ist bei Erstellung der Subscription die E-Mailadresse der Empfänger anzugeben sowie festzulegen, bei welchen Alarmen die Administratoren per E-Mail informiert werden sollen.

SCEP-Client auf Endgeräten

Nachdem der SCEP-Client auf den Endgeräten verteilt wurde, taucht auf den Clients und Servern in der Taskleiste ein neues Symbol auf. Abhängig von den Einstellungen in den Antimalware Policies der SCCM-Verwaltungskonsole können Benutzer und Administratoren Einstellungen des SCEP-Clients verändern und zum Beispiel manuell einen Quick oder Full Scan des Endgeräts starten oder ein Update der Malware-Definitionsupdates durchführen und sich über das Ergebnis des Malware Scans auf der Registerkarte "History" informieren.

Best Practices anwenden

Bei der Implementierung von SCEP 2012 sollten Sie nach dem KISS (Keep it small

Bild 4: Die SCCM-Verwaltungskonsole eröffnet auf einen Blick den Sicherheitsstatus der Client-Infrastruktur

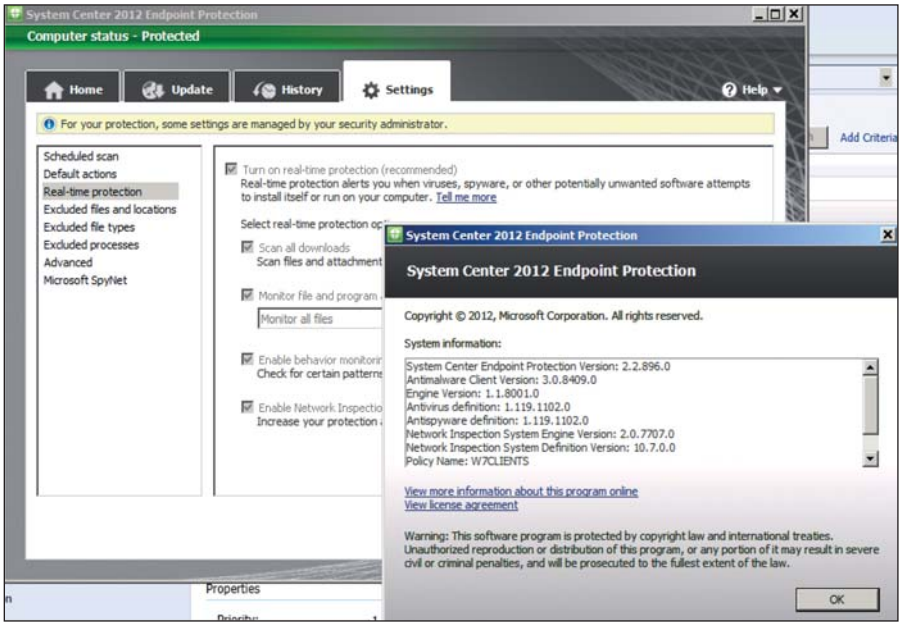


Bild 5: Über den SCEP-Client kann der Nutzer eigenständig Virenscans initiieren oder sich über den Stand der Virendefinitionen informieren

and simple)-Prinzip arbeiten. Grundsätzlich bieten sich zwei Wege zur Verteilung der SCEP-Richtlinien an:

- Verteilung anhand bestehender SCCM-Sammlungen
- Erstellung neuer SCCM-Sammlungen für SCEP

Verteilung anhand bestehender SCCM-Sammlungen

Diese Option bietet sich an, wenn Unternehmen bereits SCCM einsetzen und SCCM-Sammlungen basierend auf den Unternehmensanforderungen erstellt haben und sich gleichartige Systeme in den Sammlungen befinden. Die SCEP-spezifischen Einstellungen können somit einfach auf die bestehenden Sammlungen angewendet werden und Sie müssen lediglich das Rollout der Richtlinien abwarten, um anschließend im SCCM-Monitoring das Ergebnis des SCEP-Rollouts und das Ergebnis der Malware-Scans zu verfolgen.

Erstellen neuer SCCM-Sammlungen

Die Erstellung neuer SCCM-Sammlungen bietet sich an, wenn Unternehmen SCEP 2012 im Rahmen einer neuen SCCM 2012-Implementierung einführen und den SCCM 2012 fast ausschließlich für die System Center 2012 Endpoint Protection verwenden wollen. Hier hat es sich bewährt, SCCM-Sammlungen basierend auf Active Directory-Gruppen zu erstellen. Die Active Directory-Gruppen enthalten dann alle funktionsspezifischen Server und Clients, denen Sie dann die entsprechenden SCEP-Richtlinien zuweisen.

So etwa können Sie im Active Directory eine Sicherheitsgruppe mit dem Namen "SCEP-Exchange" erstellen und alle Exchange-Server des Unternehmens zum Mitglied der Sicherheitsgruppe machen. In der SCCM-Verwaltungskonsole schaffen Sie dann eine SCCM-Sammlung anhand der Gruppenmitgliedschaft und weisen die SCEP-Richtlinie für Exchange Server dieser Sammlung zu. Bei der Installation neuer Exchange-Server müssen Sie diese dann nur noch in die Active Directory-Gruppe aufnehmen. Die Installation des SCCM- und SCEP-Clients sowie die Zuweisung der SCEP-Richtlinie erfolgt dann automatisch.

Troubleshooting

Die Fehleranalyse in einer SCCM-Umgebung kann aufgrund der komplexen Architektur sehr umfangreich und zeitaufwändig sein. Neben den in der SCCM-Verwaltungskonsole integrierten Überwachungsmöglichkeiten des Standort- und Komponenten-Status stehen zahlreiche SCCM-Logdateien für die erweiterte Fehlersuche zur Verfügung. Die Logdatei *CCM.LOG* bietet eine Übersicht über die Client Configuration Manager Tasks. Die Datei *SMSEXEC.LOG* liefert eine Übersicht über alle SCCM-Standortserverkomponenten, um nur einige Logdateien zu nennen. Clientseitig stehen ebenfalls diverse Logdateien wie die Datei *CCMEXEC.LOG* zur Verfügung, die sämtliche SCCM-Clientaktivitäten des lokal installierten SMS Agent Host protokolliert. Die Logdateien befinden sich standardmäßig im Verzeichnis "C:\Windows\CCM\Logs". Aktivitäten von SCEP werden im Verzeichnis "C:\ProgramData\Microsoft\Microsoft Security Client\Support" gespeichert. Für die Protokollierung der SCEP-Clientaktivitäten sind die Datei *EPPSETUP.LOG*, die die SCEP-Aktivitäten festhält, und die Logdateien im Format MSSECURITY*.* von Interesse, in welchen die Antimalwareservice-Aktivitäten protokolliert werden.

Fazit

Mit der System Center 2012 Endpoint Protection geht Microsoft den konsequenten Weg, die Endpoint Protection in die System Center Produktfamilie zu integrieren. Die vorliegende Release Candidate Version zeigt die enge Integration von SCEP 2012 in den System Center Configuration Manager 2012, die es Firmen mit einer SCCM 2012-Implementierung auf einfache Weise ermöglicht, für Clients und Server für einen umfassenden Antivirus-Schutz zu sorgen und diese mit Hilfe von bekannten SCCM-Techniken zu verteilen und zu überwachen. Zahlreiche neue Funktionen machen den Umstieg auf SCEP 2012 für viele Unternehmen attraktiv. *(ln)*

[1] Neuerungen in System Center 2012 Endpoint Protection
C7P31

[2] Überblick zu System Center 2012 Endpoint Protection
C7P32

[3] Überblick zu System Center Configuration Manager 2012
C7P33

[4] System Center Configuration Manager 2012 Deployment
C7P34

Link-Codes

Anwendungen unter Windows 7 und Server 2008 R2 mit Applocker kontrollieren

Ordnung im Applikationsgehege

von Thomas Joos

In Windows 7 können Anwender auch ohne Administratorrechte verschiedene Programme installieren. Auch das direkte Starten von Anwendungen über ausführbare Dateien und USB-Sticks ist problemlos möglich – ein Einfallstor für unsichere Software sowie Spiele oder verseuchte Anwendungen. Applocker soll Administratoren daher ein Beschränken des Anwendungszoos auf Clients ermöglichen. Ein weiterer Nutzen liegt im Sperren nicht lizenzierter Anwendungen. Die Funktion ist lokal verfügbar und lässt sich auch über Gruppenrichtlinien steuern. Wie das geht, lesen Sie in diesem Workshop.

Windows 7 beherrscht Applocker in den Editionen Enterprise und Ultimate. Andere Editionen, auch die Professional Edition, können keine Anwendungen über Applocker sperren. Außerdem ist Applocker in den Editionen Standard, Enterprise und Datacenter von Windows Server 2008 R2 enthalten. Hier lassen sich nicht nur Regeln für Applocker umsetzen, sondern auf Basis von Gruppenrichtlinien auch Regeln erstellen. Am besten geben Sie Applocker-Richtlinien als Gruppenrichtlinie in Windows Server 2008 R2 vor und verteilen die Einstellungen auf diesem Weg. Rechner, die nicht kompatibel zu Applocker sind, werden nicht eingeschränkt, sondern setzen die entsprechenden Regeln einfach nicht um. Natürlich lassen sich auch lokal Einstellungen vornehmen. Diese sind allerdings nur für einzelne, wenige oder Rechner ohne Active Directory sinnvoll. Die Funktionen sind übrigens auch in Windows 8 verfügbar. Das heißt, die Regeln lassen sich bei einer Migration von Windows 7 / Windows Server 2008 R2 zu Windows 8 weiterhin verwenden. Welche Editionen von Windows 8 allerdings Applocker beherrschen, ist noch nicht sicher. Es dürfte jedoch wahrscheinlich sein, dass Microsoft hier nichts grundlegend ändern wird.

Gründliche Planung notwendig

Bevor Sie sich an das Sperren von Anwendungen machen, ist es sehr empfehlenswert, Applocker ausführlich zu testen. Durch zu straffe Regeln sperren Sie ansonsten schnell Anwendungen aus, die Ihre Anwender benötigen. Applocker zeigt sich sehr flexibel: Sie können auf Basis der Anwendung Richtlinien erstellen, die bestimmte Programme zulassen und alle anderen verweigern; oder Sie gehen den umgekehrten Weg und sperren nur unerlaubte Programme oder Software-Hersteller. Die beiden Regeln lassen sich auch miteinander mischen. Auf Basis von Gruppenrichtlinien können Sie außerdem mehrere Regelsätze erstellen und verschiedenen Benutzern oder Computern zuordnen. Wer Applocker noch tiefgehender im Unternehmen einsetzen will, kann sogar einzelne DLL-Dateien sperren lassen. Auch das Filtern auf Basis von Sicherheitsgruppen ist möglich. Administratoren können zum Beispiel einer bestimmten Sicherheitsgruppe die Installation von verschiedenen Anwendungen erlauben, für andere Sicherheitsgruppen aber nicht. So lassen sich Softwareinstallationen einfach durch Mitgliedschaften in Gruppen delegieren, erlauben oder verweigern.

Neben Gruppenrichtlinien können Sie viele Einstellungen von Applocker über PowerShell-Skripte vorgeben und über Cmdlets steuern. Dazu müssen Sie in der PowerShell mit *import-module applocker* die entsprechenden Cmdlets laden. Eine Liste der verschiedenen Cmdlets erhalten Sie mit *get-command *applocker**. Für die Befehle lassen Sie sich Hilfen und Beispiele anzeigen, wenn Sie *get-help Cmdlet* eingeben. Ausführlichere Anleitungen dazu finden Sie im Blog der Entwickler [1].

Microsoft bietet verschiedene Dokumente zur Planung und Umsetzung zum Download [2] an. Auch im Microsoft TechNet finden sich Anleitungen zum Thema [3]. Ein Video [4], das ebenfalls bei der Einrichtung hilft, finden Sie auf der Internetseite WindowsSecurity.com. Bevor Sie Applocker produktiv im Un-

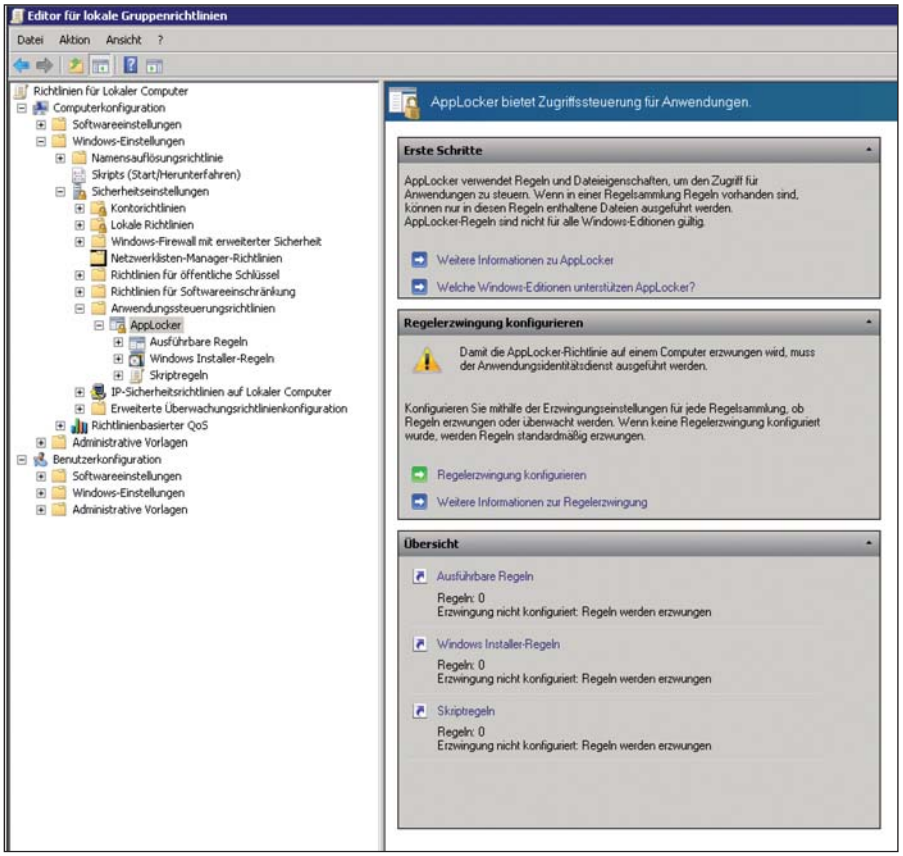


Bild 1: Beim Erstellen von Anwendungsregeln mit Applocker stehen Ihnen drei Regeltypen zur Auswahl

ternehmen einsetzen, sollten Sie diese Dokumente durcharbeiten. Erstellen Sie Applocker-Regeln, setzen die Computer und Benutzerkonten diese um, unabhängig davon, woher die Anwendung kommt, die ein Anwender starten will. Es spielt keine Rolle, ob die entsprechenden Anwender die Programme von einem USB-Stick aus starten, herunterladen, per CD ins Unternehmen bringen oder von einer anderen Quelle installieren oder starten wollen. Applocker setzt auf dem entsprechenden Computer direkt die Regeln um.

Gruppenrichtlinien für Applocker erstellen

Applocker kann nicht nur die Installation oder das Ausführen von Programmen verhindern, sondern auch bereits vorhandene Tools und Bordmittel in Windows sperren, zum Beispiel Spiele oder unerlaubte Anwendungen. Applocker baut wie erwähnt auf Regeln auf, die Sie erstellen und einer Gruppenrichtlinie zuordnen. Die Richtlinien wiederum ordnen Sie dann den Domänen oder einzelnen Organisationseinheiten zu. Die Zuordnung, welche Benutzer oder Gruppen die Regeln umsetzen, findet allerdings nicht nur über die Zuweisung der Gruppenrichtlinie, sondern bereits in der erstellten Regel in Applocker statt. Dies macht die Verwendung der Funktion extrem flexibel. Um Einstellungen per Gruppenrichtlinie an die PCs, Server oder Benutzerkonten in Ihrem Netzwerk weiterzugeben, ist es am besten, immer nach der gleichen Vorgehensweise zu verfahren:

1. Planen Sie das Anlegen der Richtlinie, in diesem Beispiel der Applocker-Regeln.
2. Legen Sie die OUs fest, auf die Sie die Richtlinie anwenden möchten. Sie können über diesen Weg auch die Zuteilung von Applocker-Regeln steuern, nicht nur in Applocker direkt.
3. Erstellen Sie die GPOs. Durch das Erstellen wendet noch kein Rechner die Einstellungen an. Erst wenn Sie die Einstellungen setzen und die GPOs mit Organisationseinheiten oder Domänen verknüpfen, wenden Computer die Richtlinien an.

Die erste Aufgabe bei der automatischen Weitergabe einer Einstellung durch eine Gruppenrichtlinie besteht darin, diese zu planen und die Organisationseinheiten festzulegen, der Sie die Richtlinie zuteilen wollen. Um ein neues GPO zu erstellen, starten Sie die Gruppenrichtlinienverwaltung, klicken in der GPMC auf den Knoten "Gruppenrichtlinienobjekte" und wählen im Kontextmenü den Befehl "Neu" aus. Geben Sie danach dem GPO einen passenden Namen, der wiedergibt, welche Einstellungen Sie mit diesem GPO verteilen. In diesem Beispiel "Applocker-Einstellungen".

Auch wenn Sie Einstellungen im GPO vornehmen und Applocker-Regeln erstellen, wendet kein Benutzer und Computer diese an. Sie müssen Ihr neues GPO erst verknüpfen. Der nächste Schritt besteht daher im Bearbeiten der Gruppenrichtlinie und dem Setzen der Einstellungen, die Sie an die Arbeitsstationen verteilen wollen. Klicken Sie im Menü "Gruppenrichtlinienobjekte" mit der rechten Maustaste auf das neu erstellte GPO und wählen Sie im Kontextmenü die Option "Bearbeiten" aus. Damit öffnet sich der Gruppenrichtlinienverwaltungs-Editor, mit dessen Hilfe Sie die Einstellungen innerhalb des GPOs vornehmen. Der Gruppenrichtlinienverwaltungs-Editor besteht aus zwei Teilen. Auf der linken Seite wählen Sie aus, für welchen Bereich Sie Einstellungen vornehmen wollen. Rechts sind dann die entsprechenden Einstellungen verfügbar.

- Die Einstellungen unter "Computerkonfiguration" wenden PCs unabhängig vom angemeldeten Benutzer an.
- Die Einstellungen unter "Benutzerkonfiguration" wenden Computer auf Benutzereinstellungen an, wenn sich Benutzer anmelden.

Applocker-Regeln in einer Gruppenrichtlinie hinterlegen

Haben Sie eine neue Gruppenrichtlinie erstellt, können Sie in dieser die entsprechenden Regeln für Applocker hinterlegen. Öffnen Sie die Bearbeitung der entsprechenden Richtlinie und navigieren Sie zu "Computerkonfiguration / Richtlinien / Windows-Einstellungen / Sicherheitseinstellungen / Anwendungssteuerungsrichtlinien". Klicken Sie nun auf "AppLocker". In diesem Bereich erstellen Sie die verschiedenen Regeln, die Applocker verwenden soll. Sie haben dabei drei Möglichkeiten, unerwünschte Programme auf den Clientcomputern zu sperren:

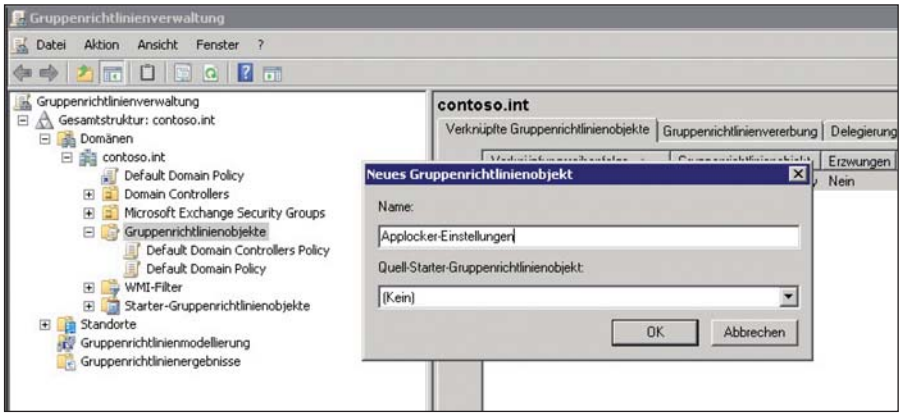


Bild 2: Achten Sie beim Erstellen einer neuen Gruppenrichtlinie für Applocker-Einstellungen auf einen aussagekräftigen Namen

1. Unter "Ausführbare Regeln" erstellen Sie Regeln für das Erfassen von Dateien mit den Endungen *.exe und *.com.
2. "Windows Installer-Regeln" legen fest, welche Anwendungen Benutzer auf dem Computer installieren dürfen. Diese Regeln erfassen Dateien mit den Endungen *.msi und *.msp.
3. Über "Skriptregeln" sperren Sie Skripte. Hier berücksichtigt Applocker Dateien mit den Endungen *.js, *.ps1, *.vbs, *.cmd und *.bat.

Sie können auch mehrere Regelsätze und alle Optionen zum Sperren von Anwendungen in einer einzelnen Gruppenrichtlinie einsetzen. So sperren Sie entweder alle Programme und erlauben nur einige über Regeln (Whitelists) oder Sie erlauben alle Anwendungen und sperren nur einzelne Programme (Blacklists). Beide Arten von Listen erlauben Ausnahmen für einzelne Programme, die Sie in den Regeln erstellen. In sicheren Umgebungen ist daher zunächst die generelle Verweigerung aller Anwendungen am effizientesten. Verweigerungs-Regeln überschreiben die Zulassungs-Regeln immer. Verweigern Sie allen Benutzern die Ausführung von Photoshop, können Sie keine Regel mehr erstellen, die einer bestimmten Gruppe die Ausführung erlaubt. In diesem Fall müssen Sie festlegen, dass nicht alle Anwender in der Programmnutzung eingeschränkt sind.

Erlauben Sie mit einer Regel allen Benutzern alle Programme, können Sie als Ausnahme Photoshop hinterlegen. In diesem Fall sperren Sie über eine Zulassungs-Regel nur Photoshop und erlauben über eine zweite Regel die Ausführung von Photoshop für eine bestimmte Gruppe. Applocker unterstützt bei diesen Vorgängen natürlich auch Gruppen im Active Directory. Erstellen Sie eine neue Applocker-Regel, hinterlegen Sie Assistenten für die Regel die Benutzergruppe. Später können Sie dann die Ausführung von Programmen über die Gruppenmitgliedschaft steuern, ohne die Applocker-Regeln neu erstellen oder ändern zu müssen.

Ausführbare Regeln einsetzen

Sogenannte "Ausführbare Regeln" für Programme sind der beste Weg für einen Einstieg in Applocker. Das Erstellung der Regeln erfolgt über einen Assistenten. Klicken Sie mit der rechten Maustaste auf "Ausführbare Regeln" und wählen Sie im Kontextmenü "Neue Regel erstellen" aus. Geben Sie auf der Seite "Berechtigungen" an, ob die Regel Anwendungen zulassen oder verweigern soll und wählen Sie im Dropdown-Menü die Gruppe aus, auf die Sie diese Regel anwenden wollen. Auf der nächsten Seite legen Sie fest, auf welcher grundlegenden Basis Applocker die Programme der Regel erfassen soll. Hier stehen Ihnen drei verschiedene Möglichkeiten zur Auswahl. Sie müssen sich für eine Option entscheiden, können aber problemlos weitere Regeln für die gleiche Gruppe auf Basis einer anderen Option erstellen:

1. Herausgeber: Durch diese Auswahl können Sie Anwendungen auf Basis ihres Zertifikats filtern. Dazu muss die Anwendung jedoch digital signiert sein. Bei Standardsoftware ist dies oft der Fall, beim Einsatz selbst entwickelter Software funktioniert das nicht immer. Diese Auswahl ist ideal, da Sie sich von Benutzern nur schwer aushebeln lässt. Stellen Sie im Vorfeld aber sicher, ob die entsprechenden Anwendungen auch signiert sind.
2. Pfad: Mit dieser Auswahl filtern Sie alle Programme in einem bestimmten Verzeichnis. Verschiebt ein Benutzer das Programm in ein anderes Verzeichnis, funktioniert die Regel nicht mehr. Diese Variante ist daher nur selten sinnvoll.
3. Dateihash: Diese verwendet den Hash-Wert einer Datei. Dieser ändert sich aber bei neuen Programmversionen. Sie müssen die Regel ändern, sobald die entsprechende Anwendung im Unternehmen aktualisiert wird. Sinnvoll ist die Auswahl unter Umständen für nicht signierte Anwendungen, die auch nicht so häufig aktualisiert werden.

Die weiteren Fenster unterscheiden sich abhängig von Ihrer vorherigen Auswahl. Verwenden Sie die Option "Herausgeber", erscheinen auf der nächsten Seite die Applikations-Filtermöglichkeit und weitere Feineinstellungen. Zunächst wäh-

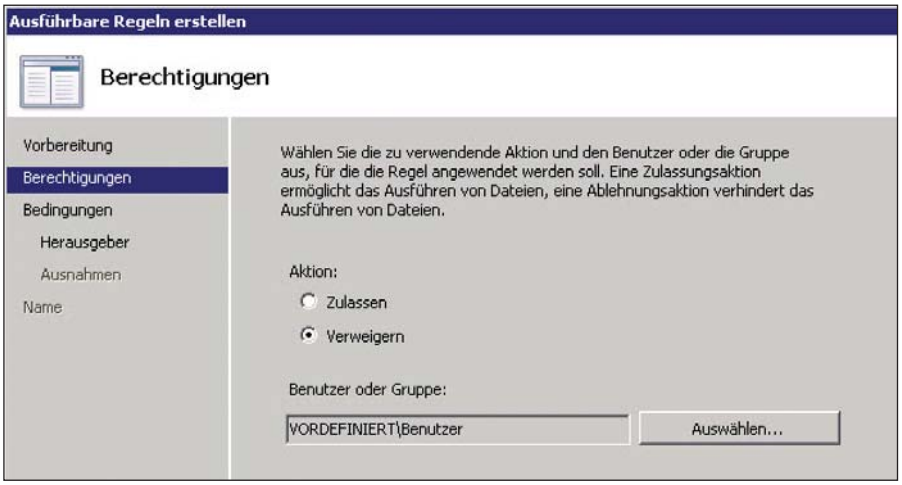


Bild 3: Das Auswählen der Benutzer und der Aktion für eine neue Applocker-Regel

Vorteilspreis für IT-Administrator Abonnenten

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Training VMware Best Practice

München, 03. September 2012 – Frankfurt/Dietzenbach, 10. September 2012

Quelle: Dan Barbalata - 123RF

Themen des Trainings:

VMware vSphere: So läuft's rund. Praxis aus 13 Jahren
- Strategien zum Aufbau einer vSphere-Umgebung
- Netzwerk und -Storagekonfigurationen im Überblick
- Sicherheit und Sicherung
- Was läuft in den virtuellen Maschinen? Best Practices der Anwendungen
- Virtuelle Desktops betreiben
- Lieblingsfehler und Troubleshooting
- Ausblick: Management, Automatisierung, Abrechnung aus der Cloud

Wiederbelebung: Disaster Recovery für virtuelle Maschinen
- Erfolgreiche Backup-Strategien
- Produkte am Markt

Monitoring und Analyse
- vSphere-Umgebungen performant und aktiv halten
- Monitoring- versus Analyseprodukte
- Tools und Produkte am Markt
- Demo: opvizor – der tägliche Healthcheck

Termin: 03. September 2012
Ort: ExperTeach Training Center München, Wredestr. 11, 80335 München

Uhrzeit: 10.00 bis ca. 17.30 Uhr

Anmeldeschluss: 24. August 2012

Termin: 10. September 2012
Ort: ExperTeach Trainingscenter Frankfurt/Dietzenbach, Waldstrasse 94, 63128 Dietzenbach

Uhrzeit: 10.00 bis ca. 17.30 Uhr

Anmeldeschluss: 31. August 2012

Trainings-Partner:

ExperTeach

Teilnahmegebühren:
Für IT-Administrator Abonnenten Euro 145,- (zzgl. 19% MwSt.), für Nicht-Abonnenten Euro 195,- (zzgl. 19% MwSt.).
Die Teilnehmerzahl ist auf 25 begrenzt.

Mehr Infos und Anmeldeformulare unter

www.it-administrator.de/workshops/

len Sie die betreffende Anwendung des Herstellers aus. Anschließend legen Sie die Version des Programms fest, das Sie mit der Regel erfassen wollen. Sie haben hier auch die praktische Möglichkeit, bestimmte Versionen von Programmen zu sperren, zum Beispiel veraltete Versionen des Internet Explorers. Aktivieren Sie die Option "Benutzerdefinierte Werte verwenden", können Sie genau bestimmen, ab oder bis zu welcher Version Sie das Programm mit Ihrer Regel erfassen wollen.

Auf der nächsten Seite legen Sie fest, ob Sie bestimmte Ausnahmen für die Regel einrichten wollen. Anschließend erhalten Sie noch eine Zusammenfassung und können eine Beschreibung für die Regel festlegen. Ihre Einstellungen können Sie auch jederzeit nachträglich anpassen. Beim Erstellen der ersten Regel erhalten Sie auch die Möglichkeit, Standardregeln anzulegen. Diese erscheinen anschließend im Fenster und Sie können diese ebenfalls nachträglich bearbeiten oder entfernen. Die Regeln erlauben zum Beispiel das Ausführen von bestimmten Programmen für Administratoren. Haben Sie alle Regeln fertig konfiguriert, die Sie in der Richtlinie erfassen wollen, müssen Sie die GPO noch einem Container im Active Directory zuordnen.

GPOs mit einem Container verknüpfen

Damit die Applocker-Einstellungen in der Gruppenrichtlinie angewendet werden, müssen Sie diese mit einer OU oder der ganzen Domäne verknüpfen. Klicken Sie dazu in der Gruppenrichtlinienverwaltung mit der rechten Maustaste entweder auf die OU, mit der Sie dieses GPO verknüpfen wollen, oder auf die Domäne. Wählen Sie im Kontextmenü die Option "Vorhandenes Gruppenrichtlinienobjekt verknüpfen" aus. Es öffnet sich ein Fenster mit allen vorhandenen Gruppenrichtlinien. Wählen Sie das GPO aus und bestätigen Sie mit "OK". Nach der Auswahl erscheint die Verknüpfung des GPOs unterhalb des Containers. Sie können das GPO auch mit mehreren OUs verknüpfen. Nehmen Sie später eine Änderung in der Regel an dem GPO vor, übernehmen alle Computer in den entsprechenden OUs die Regel. In der Gruppenrichtlinienverwaltung erkennen Sie durch die Baumstruktur unter jedem Container, welche Gruppenrichtlinien verknüpft sind. Ab diesem Moment ist das GPO aktiv. Sie können Gruppenrichtlinien auch per Drag & Drop mit dem entsprechenden Container verknüpfen. Die Umsetzung von Applocker-Richtlinien testen Sie am besten durch einen Neustart oder indem Sie *gpupdate /force* in einer Eingabeaufforderung mit Administratorrechten eingeben.

Für eine erweiterte Analyse der Anwendung einer Applocker-Richtlinie laden Sie auf der Seite SDMSoftware [5] das kostenlose Cmdlet "Group Policy Help" herunter. Nachdem Sie das Cmdlet installiert haben, können Sie mit dem Befehl *Get-SDMGPHealth -computer Computername* überprüfen, ob Gruppenrichtlinien sowie die Richtlinien für Applocker funktionieren. Auf diesem Weg schließen Sie Probleme bei Applocker-Regeln auf Grundlage falsch angewendeter Gruppenrichtlinien aus. Nach dem Download installieren Sie das Tool zunächst. Im nächsten Schritt müssen Sie noch eine DLL-Datei des Cmdlets registrieren. Gehen Sie folgendermaßen vor:

1. Öffnen Sie eine Befehlszeile und navigieren Sie zu "C:\Windows\Microsoft.NET\Framework64\v2.0.50727". Verwenden Sie ein 32 Bit-System, müssen Sie in das Verzeichnis "C:\Windows\Microsoft.NET \ Framework" wechseln.
2. Geben Sie den Befehl *installutil "C:\Programm Files (x86)\SDM Software\Group Policy Health CMDlet\GetSdmGPHealth.dll"* ein. Achten Sie aber darauf, dass der Befehl nur in Eingabeaufforderungen funktioniert, die Sie mit Administratorrechten gestartet haben.
3. Rufen Sie das "Launch PowerShell with GP Health Snap-In" in der Programmgruppe "SDM Software" auf. Im Verzeichnis "C:\Program Files (x86)\SDM Software\Group Policy Health Cmdlet" finden Sie eine Hilfedatei zum Cmdlet.
4. Mit *Get-SDMGPHealth -computer Computername* erhalten Sie den Status des Computers und dessen umgesetzte Richtlinien. Stellen Sie sicher, dass die Applocker-Richtlinie angewendet wird. Funktioniert eine Regel nicht, liegt das nicht an der Richtlinie, sondern an der Regel innerhalb der Richtlinie, wenn der Zielcomputer diese anwendet.

Gruppenrichtlinien erzwingen

In größeren Umgebungen können sich Richtlinien überschneiden und Sie können die Ausführung bestimmter Richtlinien beispielsweise deaktivieren. Haben Sie eine Richtlinie erstellt und verknüpft, klicken Sie den Container in der Gruppenrichtlinienverwaltung an. Auf der rechten Seite sehen Sie alle Gruppenrichtlinien, die mit dem Container verknüpft sind. Die neu erstellte Richtlinie für Applocker sollte hier ebenfalls erscheinen. Sie

Bild 4: Die Auswahl der Filteroptionen für ein Programm erfolgt mit einem Schieberegler

Bild 5: Mit dem Cmdlet get-sdmgphealth überprüfen Sie Computer auf angewendete Gruppenrichtlinien

haben an dieser Stelle die Möglichkeit, die Reihenfolge der Richtlinien anzupassen, in der Computer diese anwenden sollen. Um darüber hinaus sicherzustellen, dass die Applocker-Richtlinie zwingend auch in allen untergeordneten OUs angewendet wird, erzwingen Sie die Einstellungen dieser Richtlinie. In diesem Fall können untergeordnete Organisationseinheiten die Durchsetzung dieser Gruppenrichtlinie nicht verhindern. Sie erzwingen eine Gruppenrichtlinie, indem Sie auf der rechten Seite der Gruppenrichtlinienverwaltung auf der Registerkarte "Verknüpfte Gruppenrichtlinienobjekte" die Verknüpfung mit der rechten Maustaste anklicken. Wählen Sie im daraufhin geöffneten Kontextmenü die Option "Erzwungen" aus.

Nach der Auswahl erscheint eine Meldung, in der Sie das Erzwingen der Richtlinie bestätigen müssen. Wenn Sie anschließend in der GPMC eine untergeordnete OU anklicken, sehen Sie auf der rechten Seite in der Registerkarte "Gruppenrichtlinienvererbung", dass die Richtlinie auch hier als "Erzwungen" angezeigt wird. Das heißt, die Anwendung dieser Richtlinie kann nicht verhindert werden.

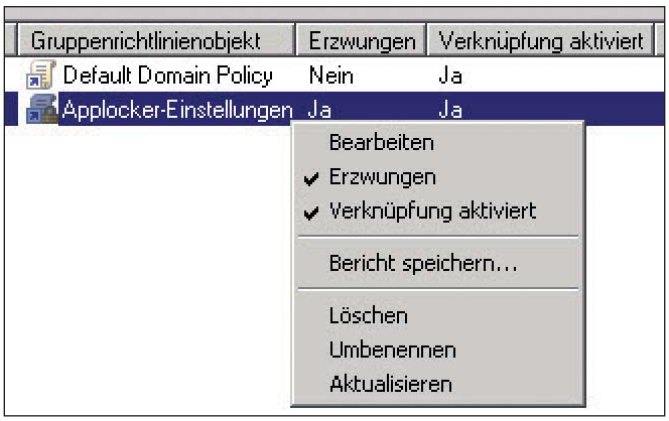


Bild 6: Das Erzwingen einer Gruppenrichtlinie in der Gruppenrichtlinienverwaltung setzt diese dann auch zwangsweise um

Regeln automatisiert erstellen

Zusätzlich zu den Möglichkeiten, Applocker-Richtlinien in Gruppenrichtlinien umzusetzen und manuell zu erstellen, können Sie Applocker auch veranlassen, automatisch Regeln für bestimmte Anwendungen zu erstellen. Dazu legen Sie ein Verzeichnis fest, das Applocker regelmäßig überwachen soll. Dieses Verzeichnis scannt Applocker automatisch und nimmt ausführbare Dateien automatisch in die Regeln auf. Klicken Sie zum Erstellen einer automatischen Regel mit der rechten Maustaste auf "Ausführbare Regeln" und wählen Sie die Option "Regeln automatisch generieren". Geben Sie im Assistenten das Verzeichnis an, das Applocker einbinden soll, sowie die Benutzergruppe, für die Sie die Regel anwenden wollen. Als Nächstes wählen Sie aus, auf welcher Basis Applocker die Regel erstellen soll. Auch hier haben Sie die Möglichkeit, Herausgeber, Datei-Hash oder Pfad zu verwenden. Ähnliche Dateien lassen sich in gemeinsamen Regeln zusammenfassen. Auf der nächsten Seite erhalten Sie eine Zusammenfassung und können die automatisch erstellten Regeln anzeigen lassen. Auf Basis der Auswahl erstellt der Assistent Zulassungsregeln für die gefundenen Programme. Wie bei den manuellen Regeln können Sie auch hier Einstellungen nachträglich anpassen.

Klicken Sie auf "Applocker" im linken Bereich der Konsole, haben Sie die Möglichkeit, auf der rechten Seite die Option "Regelerzwingung konfigurieren" auszuwählen. Es öffnet sich ein neues Fenster, in dem Sie festlegen, wie sich Applocker bei den verschiedenen Regeln verhalten soll. Aktivieren Sie zum Beispiel für einen Regelbereich die Option "Konfiguriert", können Sie im Dropdown-Menü Einstellungen ändern. Aktivieren Sie "Regeln erzwingen" oder die Einstellung "Nur überwachen". Im Überwachungs-Modus setzt Applocker die Regeln nicht um, sondern protokolliert nur die betroffenen Anwendungen. Sie finden die Meldungen in der Ereignisanzeige über "Anwendungs- und Dienstprotokolle / Microsoft / AppLocker".

Auf der Registerkarte "Erweitert" aktivieren Sie schließlich bei Bedarf die DLL-Regeln. Danach finden Sie im linken Bereich die neue Option "DLL-Regeln". Hier erstellen Sie Applocker-Regeln auf Basis von DLL-Dateien. Diesen Bereich sollten Sie aber erst dann verwenden, wenn es bereits eine Applocker-Infrastruktur gibt. DLL-Regeln erstellen Sie genauso wie Regeln über ausführbare Dateien. Der Unterschied dabei ist nur, dass Sie keine COM- oder EXE-Dateien auswählen, sondern DLL-Dateien, welche die Regel erfassen soll. Auch hier können Sie bestimmte Versionen sperren, erlauben oder filtern wie bei ausführbaren Regeln. *(dr)*

Link-Codes

[1] Applocker Entwickler-Blog
C5P41

[2] Planung und Umsetzung von Applocker
C5P42

[3] TechNet-Anleitung zu Applocker
C5P43

[4] Video zur Applocker-Einrichtung
C5P44

[5] Download Cmdlet "Group Policy Help"
C5P45

Open Source-Identity-Management mit FreeIPA

Offene Quelle, geschlossenes Ziel

von Thorsten Scherf

Single Sign On-Lösungen gibt es im Linux-Umfeld schon recht lange. Mit FreeIPA steht allerdings eine Lösung zur Verfügung, die nicht nur viele bekannte Open Source-Tools unter einem Dach vereint, sondern auch besonders einfach und effizient zu bedienen ist – unter anderem dank eines übersichtlichen Webinterfaces. Wie Sie FreeIPA aufsetzen und welche neuen Features die aktuelle Version 2.2 bietet, erfahren Sie in diesem Workshop.


Quelle: Oleg Romanciuk - 123RF

IPA, das steht für Identity, Policy und Audit. Mit Version 2.0 des Open Source-Identity-Management-Systems wurde bereits das Identity-Management für Benutzer, Maschinen und Services eingeführt. Mit der seit April aktuellen Version 2.2 kommen neue Funktionen für den Bereich Policy hinzu. Das noch recht junge Projekt FreeIPA [1] vereint dabei diverse bekannte Open Source-Tools unter einer Haube und spendiert diesen ein einfach zu bedienendes Webinterface und ein entsprechendes Kommandozeilentool. Zu den integrierten Tools zählen beispielsweise der 389 LDAP-Server [2], das Dogtag PKI-System [3], das MIT Kerberos [4] sowie der ISC DHCP- und DNS-Server [5,6]. Um auf allen Systemen für eine einheitliche Uhrzeit zu sorgen, steuert das NTP-Projekt den beliebten Zeitserver [7] bei. FreeIPA sorgt dabei für eine entsprechende Verzahnung und korrekte Kommunikation der einzelnen Komponenten untereinander. So speichert das MIT Kerberos beispielsweise die Principal-Datenbank für Benutzer, Maschinen und Services in einer LDAP-Datenbank. Gleiches gilt auch für den BIND DNS-Server und das Dogtag-Zertifikatssystem.

Neuerungen in Version 2.2

Erstmals enthält die Version nun auch eine Unterstützung für zentrale SELinux-Richtlinien. Dabei bekommt ein Benutzer bei einer erfolgreichen Authentifizierung eine zentral gespeicherte SELinux-Rolle zugewiesen. Ein lokales Mapping ist somit nicht mehr notwendig; ein Support für Host-Based-Access-Control (HBAC) ist bereits seit der vergangenen Version verfügbar. Neu hinzu kommt, dass sich auch sudo-Regeln auf dem IPA-Server speichern lassen. Auch hier ist es nun nicht mehr notwendig, die Regeln lokal vorzuhalten. Bei einem Zugriff über sudo lädt das Client-System die Regeln automatisch vom IPA-Server nach. Auch der Identity-Bereich wurde weiter ausgebaut, so unterstützt IPA nun Maschinen- und Service-Identitäten. Dank der Integration der offenen Dogtag-PKI nun sogar mittels X.509-Zertifikaten. Das Zusammenspiel der einzelnen Komponenten zeigt Bild 1.

Die IPA-Kommandozeilen-Tools haben sich im Vergleich zur Version 1.0 geändert. Statt einer Vielzahl von unterschiedlichen Tools zu haben, existiert für die allermeisten Aufgaben nun ein zentrales Tool. Je nachdem, welches Argument Sie dem Tool übergeben, werden entsprechende Aktionen ausgeführt. Beispielsweise verwenden Sie zum Anlegen eines neuen Benutzers nun nicht mehr das Tool ipa-adduser, sondern rufen stattdessen *ipa user-add* auf. Welche Aktionen alle möglich sind, zeigt die Ausgabe von *ipa help*.

Bei der Server-Installation auf DNS achten

Bevor es an die Installation des eigentlichen FreeIPA-Servers geht, stellen Sie sicher, dass sich die Namen aller verwendeten Maschinen via DNS auflösen lassen. Erweitern Sie den vorhandenen DNS-Server um einige Service-Einträge (SRV-Records), erleichtert das später auch die Konfiguration der Client-Maschinen. Diese erhalten dann

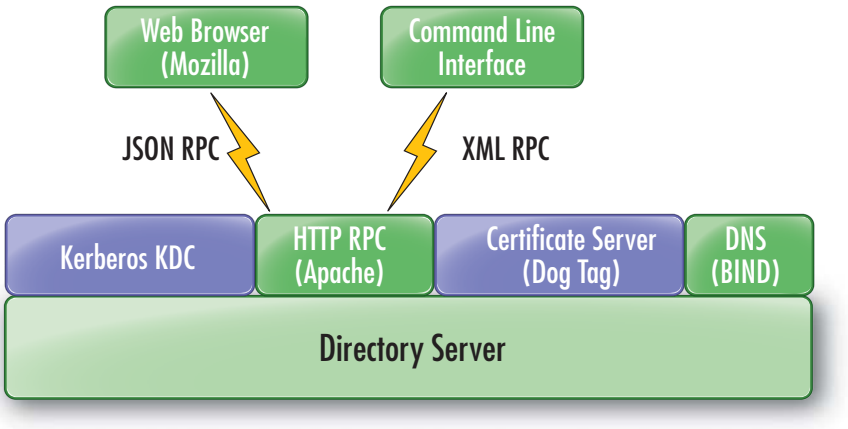


Bild 1: Bekannte Open-Source-Tools laufen bei FreeIPA unter einer Haube

über eine DNS-Abfrage Informationen über ihre zuständigen Server und den Kerberos-Realm; eine manuelle Konfiguration ist kaum mehr nötig. Bei der Installation des FreeIPA-Servers besteht optional die Möglichkeit der Installation und Konfiguration eines DNS-Servers. Da die DNS-Serverdaten wie alle anderen IPA-Daten auch im LDAP liegen, ist zwingend vor der IPA-Server-Installation das Paket bind-dyndb-ldap zu installieren. Auf einem Fedora Linux System klappt die Installation des Servers leicht mit Hilfe des Paketmanagers yum. Für andere Distributionen steht unter [8] auch eine Archiv-Datei mit den Quellen der Software zur Verfügung. Über den bekannten Dreisatz "configure, make, make install" ist im Handumdrehen auch hieraus eine lauffähige Version gebaut. Nach der Installation richten Sie die einzelnen Komponenten entsprechend ein. Dies geht sehr einfach mittels:

```
# ipa-server-install –setup-dns
```

Durch den Aufruf der Setup-Routine werden nun die folgenden Komponenten auf der Maschine installiert:

- NTP
- Fedora Directory Server
- Fedora Dogtag PKI
- MIT Kerberos
- Apache Webserver
- SELinux Policy für die diversen FreeIPA Komponenten

Das Installationsprogramm fragt dann die notwendigen Informationen wie LDAP Base DN, Kerberos Realm, Servername et cetera ab und schon nach einigen Minuten ist der Server inklusive aller Komponenten einsatzbereit. Sollte IPA innerhalb einer virtuellen Maschine laufen, bietet es sich an, die automatische Installation des NTP-Servers mittels der Option "--no-ntp" zu deaktivieren. Auch für die anderen Komponenten existiert eine Vielzahl von Optionen, die Sie dem Setup-Tool mit übergeben können. Mittels *ipa-server-install* erhalten Sie eine Übersicht aller verfügbaren Optionen. Soll die Installation des FreeIPA Servers komplett automatisiert ablaufen, beispielsweise als Teil einer Kickstart-Installation, so ist dies mit Hilfe einiger weiterer Optionen möglich:

```
# ipa-server-install –setup-dns -U
  -u ldap -r VIRT.TUXGEEK.DE -p ds-
  password -a ipa-admin-password
```

Die Option "-u" bestimmt hier den Benutzer, unter dem der FreeIPA-Server laufen soll, "-r" den Kerberos-Realm, "-p" das Passwort für den Directory Manager und "-a" das Passwort für den FreeIPA-Admin, den IPA per default erzeugt. Hat die Installation soweit geklappt, können Sie die korrekte Funktionsweise mittels *kinit admin* verifizieren. Hiermit fordern Sie ein Benutzer-Ticket vom Kerberos-Server an. Hat dies funktioniert, so zeigt *klist* das empfangene Kerberos TGT an:

```
# kinit admin
Password for admin@VIRT.TUXGEEK.DE:

# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin@VIRT.
  TUXGEEK.DE
Valid starting Expires
  Service principal
04/01/12 21:14:12  04/02/12 21:14:10
  krbtgt/VIRT.TUXGEEK.DE@VIRT.
  TUXGEEK.DE
```

Im nächsten Schritt sollten Sie die ersten Benutzerkonten anlegen. Wie bereits erwähnt funktioniert dies nun mittels *ipa user-add*. Das Tool fragt die notwendigen Attribute interaktiv ab.

```
# ipa user-add –password tscherf
First name: Thorsten
Last name: Scherf
Password:
Enter Password again to verify:
----------
Added user "tscherf"
----------
  User login: tscherf
  First name: Thorsten
  Last name: Scherf
  Full name: Thorsten Scherf
  Display name: Thorsten Scherf
  Initials: TS
  Home directory: /home/tscherf
  GECOS field: tscherf
  Login shell: /bin/sh
```

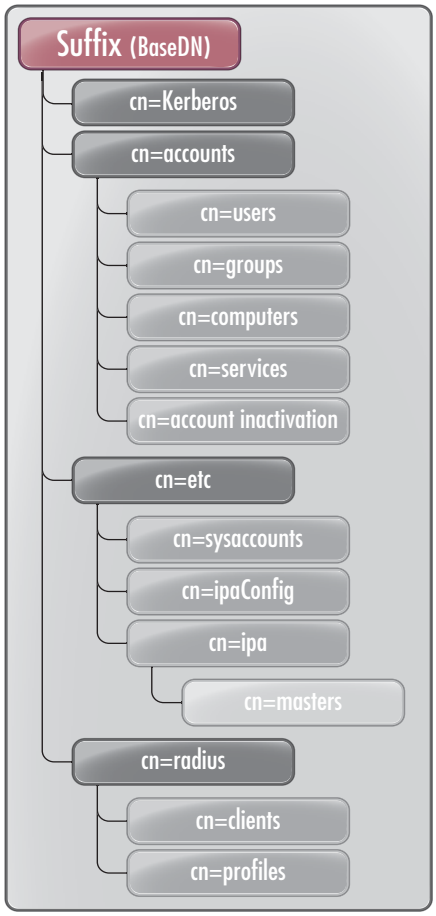


Bild 2: Der IPA LDAP-Server enthält eine Vielzahl von Containern für die einzelnen Subsysteme

```
  Kerberos principal:
  tscherf@VIRT.TUXGEEK.DE
  UID: 1215000005
```

Alternativ können Sie sämtliche Informationen für den Benutzer-Account aber natürlich auch als Optionen übergeben. Möchten Sie sämtliche Attribute für den Benutzer sehen, fragen Sie mittels *ldapsearch* einfach das Benutzer-Objekt direkt im LDAP-Baum ab:

```
# ldapsearch -Y GSSAPI -b
  dc=virt,dc=tuxgeek,dc=de -LLL
  uid=tscherf
```

Da für den Zugriff auf den LDAP-Server bereits das Kerberos-Protokoll verwendet wurde, zeigt der Aufruf von *klist* neben dem initial ausgestelltem Kerberos TGT nun auch das Service-Ticket für den Zugriff auf den LDAP-Server an:

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin@VIRT.
  TUXGEEK.DE

Valid starting Expires
  Service principal
04/01/12 21:14:12  04/02/12 21:14:10
  krbtgt/VIRT.TUXGEEK.DE@VIRT.
  TUXGEEK.DE
04/01/12 21:18:22  04/02/12 21:18:16
  HTTP/ipa1.virt.tuxgeek.de@VIRT.
  TUXGEEK.DE
04/01/12 21:18:23  04/02/12 21:18:21
  ldap/ipa1.virt.tuxgeek.de@VIRT.
  TUXGEEK.DE
```

Viele administrative Aufgaben lassen sich natürlich auch bequem über das FreeIPA-Webinterface erledigen. Hierfür ist jedoch zuerst der Webbrowser für den entsprechenden Kerberos-Realm zu konfigurieren. Beim Firefox lassen sich die aktuellen Konfigurationseinstellungen über "about:config" anzeigen. Die folgenden Anweisungen sind individuell anzupassen:

```
network.negotiate auth.trusted
  uris .virt.tuxgeek.de
network.negotiate auth.delegation
  uris .virt.tuxgeek.de
network.negotiate auth.using
  native-gsslib true
```

Sollte eine Kerberos-Verbindung zum IPA-Server fehlschlagen, so besteht in der aktuellen Version ebenfalls die Möglichkeit, eine rein Passwort-basierte Authentifizierung durchzuführen. Dies kann recht hilfreich sein, wenn der Webbrowser beispielsweise auf einer Windows-Arbeitsstation läuft und diese bereits Teil einer Windows-AD Domäne ist. Nachdem eine HTTPS-Verbindung zum FreeIPA-Server besteht, lassen sich sehr komfortabel Benutzer über das Webinterface einrichten oder abfragen.

Redundanz schaffen

Nachdem Sie die grundlegende Konfiguration des Servers abgeschlossen haben, sollten Sie die Daten des Directory-Servers auf ein zweites System replizieren. Dieses ist dann ebenfalls in der Lage, Änderungen von Clients entgegenzunehmen und sie auf den jeweils anderen Server zu replizieren. Nach Ausfall eines Masters sind die Daten nach wie vor über den anderen Master verfügbar und lassen sich dort ändern. Ist der ausgefallene Server wieder online, werden die geänderten Daten auf ihn zurückrepliziert. Auch zur Lastverteilung bietet sich der Einsatz mindestens zweier Server an. Speichern Sie die Daten an mehreren, geografisch voneinander getrennten Standorten, so sollten Sie sich überlegen, unter Umständen noch weitere Server zu konfigurieren und als Replicas einzurichten, damit nicht für jede Abfrage oder Änderung am Directory eine WAN-Verbindung nötig ist. Die Konfiguration eines Replica-Systems geht auch hier sehr schnell von der Hand. Auf dem ersten Master ist eine Konfigurationsdatei mit allen notwendigen Information für den zusätzlichen Server zu erzeugen:

```
# ipa-replica-prepare
  ipareplica.virt.tuxgeek.de
Directory Manager (existing master)
  password:

Preparing replica for
  ipareplica.virt.tuxgeek.de from
  ipa1.virt.tuxgeek.de
Creating SSL certificate for the
  Directory Server
Creating SSL certificate for the
  Web Server
Exporting RA certificate
Copying additional files
Finalizing configuration
Packaging replica information into
/var/lib/ipa/replica-info-iparepli-
  ca.virt.tuxgeek.de.gpg
```

Nun kopieren Sie einfach die so erzeugte Datei auf den Replica-Host und starten dort die Installation mittels *ipa-replica-install*. Achten Sie darauf, dass zuvor alle FreeIPA-Pakete installiert wurden:

```
# scp /var/lib/ipa/replica-info-
  ipareplica.virt.tuxgeek.de.gpg
  root@ipareplica:/var/lib/ipa/
# ipa-replica-install
  /var/lib/ipa/replica-info-
  ipareplica.virt.tuxgeek.de.gpg
```

Ist das Installationsprogramm ohne Fehler durchgelaufen, startet im Anschluss eine Replikation der LDAP-Datenbank. Fügen Sie dieser Replica nun noch ihre DNS-Zonendatei hinzu, stehen zwei unterschiedliche Server bereit. Die so eingerichteten Replizierungsvereinbarungen (replication agreements) lassen sich mittels *ipa-replica-manage* anzeigen oder auch nachträglich ändern.

Zum Thema Synchronisation sei hier noch angemerkt, dass diese im Übrigen auch zwischen einem FreeIPA-Server und einem Active Directory-Domänencontroller funktioniert. Somit stehen die Windows-Konten ebenfalls für eine Anmeldung auf Linux-Maschinen zur Verfügung. Die Konfiguration ist unter [9] beschrieben. Das Setup ist jedoch recht mühsam und erfordert die Installation von zusätzlicher Software auf den AD-Domänencontrollern. Da dies oftmals problembehaftet ist, wird an dieser Stelle nicht näher auf die Konfiguration eingegangen. Jedoch haben die Entwickler bereits angekündigt, Cross-Realm Trusts mit AD-Domänen in die FreeIPA-Version 3 einzubauen [10]. Hiermit wäre dann nach dem Setup eines Trusts zwischen der IPA- und der AD-Domäne ein Login mit Windows-Benutzerkonten auch auf Linux-Systemen möglich.

Clients konfigurieren

Ein FreeIPA-Client existiert nicht nur für Fedora und Red Hat Enterprise Li-

nux (RHEL), sondern es gibt Clients für eine Vielzahl verschiedener Unix-Varianten wie Solaris, AIX, HP-UX oder auch Mac OS X. Auf einem Fedora-System gelingt die Installation einfach mit einem Yum-Aufruf:

```
# yum install ipa-client
```

Als Administrator installieren Sie auf Ihrer Arbeitsstation zusätzlich noch das Paket ipa-admintools. Da der FreeIPA-Server auch als DNS-Server konfiguriert wurde, ist dieser nun auch auf den Client-Systemen in der Datei */etc/resolv.conf* einzutragen. Die eigentliche Konfiguration des Clients erfolgt dann über den Aufruf von *ipa-client-install*. Dank der Service-Records im DNS findet der Client sämtliche Server automatisch durch ein Service-Discovery:

```
# ipa-client-install
Discovery was successful!
Realm: VIRT.TUXGEEK.DE
DNS Domain: virt.tuxgeek.de
IPA Server: ipa1.virt.tuxgeek.de
BaseDN: dc=virt,dc=tuxgeek,dc=de

Continue to configure the system
  with these values? [no]: yes
Enrollment principal: admin
Password for admin@VIRT.TUXGEEK.DE:
Enrolled in IPA realm
  VIRT.TUXGEEK.DE
Created /etc/ipa/default.conf
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA
  realm VIRT.TUXGEEK.DE
SSSD enabled
Kerberos 5 enabled
NTP enabled
Client configuration complete.
```

Für den Host wird hierbei direkt ein Principal in der Kerberos-Datenbank auf dem FreeIPA-Server erzeugt. Dies ist wichtig, damit Sie später einen IPA-Service, wie beispielsweise einen NFS-, SSH- oder Web-Server mit einem Kerberos-Principal oder einem X.509-Zertifikat einrichten können. Alternativ hierzu lässt sich der Client auch recht leicht mit Hilfe des Tools system-comfig-authentication einrichten. Sollte der Client noch über keinen DNS-Eintrag auf dem FreeIPA-Server verfügen, holen Sie diesen Eintrag mit Hilfe des FreeIPA Kommandozeilen-Tools sehr leicht nach:

```
# ipa dns-add-rr virt.tuxgeek.de
  ipa2 A 192.168.0.23
------
dns-add-rr:
------
  dn: idnsname=ipa2,idnsname=virt.
  tuxgeek.de,cn=dns,dc=virt,
  dc=tuxgeek,dc=de
  arecord: 192.168.0.23
  objectclass: top
  objectclass: idnsrecord
----------------------------------
Added DNS resource record "ipa2 A
  192.168.0.23" to zone "virt.
  tuxgeek.de".
----------------------------------
```

Hilfreicher Security-Daemon

Der System-Security-Service-Daemon (SSSD) stellt als Client-Komponente verschiedene Funktionen zur Verfügung, wovon einige besonders interessant sind: Zum einen löst das Tool das Problem der Offline-Authentifizierung eines Benutzers. Der SSSD hält empfangene Credentials eines zentralen Servers einfach im lokalen Cache vor. Meldet sich ein Benutzer also im Firmennetzwerk mit seinem Konto an seinem Notebook an, so gelangen die Credentials automatisch in den SSSD-Cache. Wie lange diese dort liegen bleiben und gültig sind, lässt sich natürlich in einer zentralen Konfigurationsdatei festlegen.

Des Weiteren unterstützt der SSSD die Abfrage mehrerer LDAP- oder auch NIS-Server. Hiermit lässt sich dann eine Vielzahl unterschiedlicher Benutzerdatenbanken abfragen. Auch aus Performance-Sicht bietet der Einsatz des neuen Daemons einen Vorteil. Anstatt für jede Abfrage an den LDAP-Server eine eigene Verbindung aufzubauen, ist lediglich ein Socket vom SSSD selbst zum LDAP-Server notwendig. Der Daemon bietet dabei eine eigene NSS- und PAM-Schnittstelle für anfragende Client-Systeme an. Im Backend sorgen sogenannte Security-Provider für einen Zugriff auf den entsprechenden Identity- und Authentication-Server.

Da das Client-System zu diesem Zeitpunkt bereits über einen Host-Principal in der Kerberos-Datenbank verfügt, ist ein Login über die GSSAPI-Schnittstelle des SSH-Servers bereits möglich:

```
# kinit tscherf
# ssh tscherf@ipa2
Last login: Wed May 02 21:04:35 2012
  from 192.168.0.12
# id
uid=1640400005(tscherf)
  gid=1640400005(tscherf)
groups=1640400005(tscherf),164040000
  1(ipausers)
context=unconfined_u:unconfined_r:un
  confined_t:s0-s0:c0.c1023
```

Auf dem Source-System sollte die Ausgabe von *klist* nun neben dem Kerberos TGT auch das Host-Principal des Clients anzeigen.

Kerberos-Service konfigurieren

Nun geht es an die Konfiguration des ersten eigenen Kerberos-Dienstes. Als Beispiel dient ein NFS-Server, der sich von den Client-Maschinen über das sichere NFSv4-Protokoll mit Kerberos-Authentifizierung ansprechen lässt. Zusätzlich soll der Server auch für Datenintegrität und Vertraulichkeit sorgen. Hierfür richten wir auf dem IPA-Server eine NFS-Freigabe ein, die nicht nur eine Benutzerauthentifizierung auf Basis von NFSv4 durchführt, sondern auch für Datenauthentizität und Datenintegrität sorgt:

```
# cat /etc/exports
/data
  gss/krb5(rw,fsid=0,subtree_check)
/data
  gss/krb5i(rw,fsid=0,subtree_check)
/data
  gss/krb5p(rw,fsid=0,subtree_check)
```

In der Kerberos-Datenbank erzeugen Sie nun ein Service-Principal für den NFS-Dienst und exportieren die Keytab-Datei des Servers:

```
# ipa service-add nfs/ipa1.virt.
  tuxgeek.de
-----------------------------
Added service "nfs/ipa1.virt.
  tuxgeek.de@VIRT.TUXGEEK.DE"
-----------------------------
Principal:
```

```
  nfs/ipa1.virt.tuxgeek.de@VIRT.
  TUXGEEK.DE
Managed by: ipa1.virt.tuxgeek.de

# ipa-getkeytab -s ipa1 -p
  nfs/ipa1.virt.tuxgeek.de -k
  /etc/krb5.keytab
Keytab successfully retrieved and
  stored in: /etc/krb5.keytab
```

Ein *echo SECURE_NFS=yes > /etc/sysconfig/nfs* sorgt dafür, dass nach einem *service nfs start* alle notwendigen NFS-Dienste verfügbar sind. Die Client-Konfiguration verläuft ähnlich. Sie erzeugen auch ein NFS Service-Principal und speichern dieses lokal in der Datei */etc/krb5.keytab* ab:

```
# kinit admin
Password for admin@VIRT.TUXGEEK.DE:
# ipa service-add nfs/`hostname`
----------------------------
Added service "nfs/ipa2.virt.
  tuxgeek.de@VIRT.TUXGEEK.DE"
----------------------------
  Principal:
  nfs/ipa2.virt.tuxgeek.de@VIRT.
  TUXGEEK.DE
  Managed by: ipa2.virt.tuxgeek.de

ipa-getkeytab -s
  ipa1.virt.tuxgeek.de -p
  nfs/ipa2.virt.tuxgeek.de -k
  /etc/krb5.keytab
Keytab successfully retrieved and
  stored in: /etc/krb5.keytab
```

Damit die notwendigen NFS-Client Dienste rpcgssd und rpcidmapd korrekt starten, nehmen Sie auch auf dem Client den Eintrag "SECURE_NFS=yes" in der Datei */etc/sysconfig/nfs* vor. Nun sollte einem erfolgreichen NFSv4-Mount mit der höchstmöglichen Sicherheitsstufe nichts mehr im Wege stehen:

```
# echo "SECURE_NFS=yes" > /etc/
  sysconfig/nfs"
# service rpcgssd start
# mount -t nfs4 -o sec=krb5p
  ipa1.virt.tuxgeek.de:/ /mnt/
```

Schließlich bestätigt der Aufruf von *df*, dass das soeben eingebundene Dateisystem tatsächlich zur Verfügung steht:

```
# df -Th /mnt/
Filesystem Type Size Used Avail Use%
  Mounted on
ipa1.virt.tuxgeek.de:/  nfs4    3.5G
  1.5G  1.8G  46% /mnt
```

Zugangskontrollen einrichten

Seit der FreeIPA Version 2 steht nun auch der Support für Host-based-Access-Control (HBAC)-Regeln zur Verfügung. Hiermit ist es sehr leicht möglich, zu entscheiden, welcher Benutzer Zugriff auf welches System oder welchen Service bekommt. Als Standardeinstellung ist der Zugriff für alle Benutzer auf alle Maschinen und sämtliche Dienste erlaubt. Das folgende Beispiel verbietet dabei den Zugriff für den Benutzer Foo auf die Maschine ipa2.tuxgeek.de:

```
# ipa user-add foobar –first=Foo
  -last=User –password
# ipa hbacrule-add bar-deny-rule
  –type=deny –servicecat=all
  –srchostcat=all
# ipa hbacrule-add-user bar-deny-
  rule –users=foo
# ipa hbacrule-add-host bar-deny-
  rule –hosts=ipa2.tuxgeek.de
```

Der Zugriff auf das System ipa2.tuxgeek.de sollte für alle Benutzer außer Foo möglich sein. Die Regeln lassen sich auch umdrehen, dann müssen Sie allerdings zuerst die allow_all Regel entfernen:

```
# ipa hbacrule-disable allow_all
# ipa hbacrule-add deny_all
  –type=deny –usercat=all
  –hostcat=all –srchostcat=all
  –servicecat=all
```

Hiermit wäre der Zugang für alle Benutzer verboten und es müssten zuerst die gewünschten Zugriffe eingerichtet werden, bevor ein Benutzer sich auf einem System anmelden kann. Dies kann natürlich auch auf Gruppenebene erfolgen. Auch die Integration von sudo in die aktuelle FreeIPA-Version ist ein wichtiges Feature. Statt die sudo-Regelsätze dezentral über eine sudoers-Datei zu verwalten, besteht nun die Möglichkeit, diese im zentralen LDAP-Server von FreeIPA abzulegen. Wie die LDIF-Dateien, die in den LDAP-Server zu laden sind, genau auszusehen haben, können Sie unter [11] nachlesen. Nach dem Import müssen Sie dann nur noch dem Client mitteilen, dass bei einem sudo-Aufruf der LDAP-Server nach einer passenden Regel zu befragen ist.

Dies geschieht über einen entsprechenden Eintrag in der Datei */etc/nsswitch.conf*. Hier nehmen Sie in der Zeile "sudoers" mit *sudoers = files sss* einen Eintrag für den Zugriff vom SSSD auf den LDAP-Server vor. Nach einem Neustart des sssd-Dienstes ist dieser in der Lage, die sudo-Regeln in einem lokalen Cache abzulegen.

Fazit

Die aktuelle FreeIPA-Version 2.2 bietet eine Menge neuer Features. Der Bereich Policy-Management hat mit der zentralen Ablage von sudo-Regeln ein regelrechtes Killerfeature bekommen und auch die SELinux-Integration ist gelungen. Mit dem nächsten Major-Release steht die Integration von Cross Kerberos-Realm Trusts an. Damit wäre dann eine saubere Integration in bestehende Microsoft Active Directory-Domänen möglich. Die aktuelle Synchronisation von bestehenden Konten ist momentan doch etwas mühsam. *(dr)*

[1] FreeIPA Projekt C7P21
[2] 389 LDAP-Server C7P22
[3] Dogtag-PKI Projekt C7P23
[4] MIT Kerberos C7P24
[5] ISC DHCP-Server C7P25
[6] ISC DNS-Download C7P26
[7] NTP-Server Projekt C7P27
[8] FreeIPA Downloadseite C7P28
[9] Integration FreeIPA und Active Directory C7P29
[10] Cross-Realm Trusts mit AD-Domänen C7P20
[11] sudo-Integration C7P2A

Link-Codes

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

Mobile Geräte an Microsoft-Infrastrukturen anbinden

Alles dran!

von Thomas Joos

Erst die Anbindung an die Ressourcen und Daten im Unternehmen macht aus einem Smartphone oder Tablet ein vollwertiges Arbeitsmittel. Dazu ist zunächst der sichere Zugriff auf die Daten zu realisieren. Intern muss der Zugriff durch Geräte-Richtlinien gestaltet werden; erfolgt dieser von außen, bietet sich zudem ein VPN an. In einer Microsoft-basierten Infrastruktur benötigt der mobile Client zusätzlich den Zugriff auf Exchange und Sharepoint. Wie Administratoren all diese Anforderungen umsetzen und welche Zusatztools dazu notwendig sind, zeigt dieser Workshop.

Die Integration von Smartphones in Firmennetzwerke und das damit einhergehende Mobile Device Management gehören mittlerweile zu den Standardaufgaben in Unternehmen. Denn immer häufiger greifen Anwender mit Smartphones oder Tablet-PCs auf Ressourcen im Unternehmen zu. Dazu ist es wichtig, dass auf den entsprechenden Endgeräten Einstellungen so gesetzt sind, dass diese nicht nur optimal mit dem Netzwerk harmonieren, sondern auch sicher sind. Zunehmend stellen Unternehmen den Anwendern keine Geräte mehr zur Verfügung, sondern arbeiten nach dem Bring-Your-Own-Device-Prinzip, mit dem Anwender ihre privaten Smartphones unter bestimmten Umständen nutzen dürfen.

Quelle: PKDINKAR – 123RF

Administratoren müssen bei all diesen Aufgaben verschiedene Ansätze im Auge behalten, um die Geräte sicher anzubinden. Es gibt verschiedene Systeme mit unterschiedlichen Versionsständen. Vor allem Android bereitet durch seine offene Struktur teilweise Probleme. In den meisten Fällen greifen Anwender mit Smartphones über ein VPN oder veröffentlichte Server zu. Der Dateizugriff erfolgt dabei zum Beispiel über SharePoint oder Exchange.

iPhones, Android und Windows Phone im Vergleich

Der Vorteil beim Einsatz von iPhones und iPads sind zunächst die restriktiven Vorschriften bei der Installation von Anwendungen. Apps lassen sich beim geschlossenen iOS-System nur über den offiziellen App-Store installieren oder von Unternehmen zentral über das iPhone-Konfigurationsprogramm vorgeben. Unternehmen, die zahlreiche iPhones anbinden müssen, können mit dem kostenlosen iPhone-Konfigurations-Programm [1] eine zentrale Verwaltung durchführen. Das Tool ermöglicht die Erstellung, Verwaltung, Verschlüsselung und Bereitstellung von Profilen. Apps lassen sich über das Tool verteilen beziehungsweise die Installation von Apps von Drittherstellern durch Anwender verhindern. Auch die Verwendung der Kamera oder das Erstellen von Bildschirm-

Bild 1: Die unternehmensweite Konfiguration des iPhones lässt sich mit einem Apple-Tool realisieren

fotos lässt sich auf diese Weise verhindern. Über das Konfigurationsprogramm lassen sich auch Exchange-Profile oder die VPN-Anbindung vorbereiten.

Android-Geräte sind im Vergleich zu iPhones sehr offen, erweiterbar und erlauben Anwendern nahezu alle Steuerungs- und Zugriffsmöglichkeiten. Unternehmen tun aber gut daran diese Möglichkeiten einzuschränken, um zu verhindern, dass Viren ins Netzwerk geraten. Google bietet zum Beispiel mit dem kostenlosen Tool "Google Apps Device Policy" die Möglichkeit, Android-Handys mit Sicherheitsrichtlinien zu versorgen. Die Software läuft dazu auf dem Endgerät als Systemdienst und tauscht sich mit einem Google-Server aus. Über den Server lassen sich Geräte bei Verlust auch löschen (Remote Wipe). Dieses Löschen funktioniert auch über Exchange.

Android erlaubt weitgehende Freiheit für die Installation von Apps. Das lässt sich in Unternehmen auch kaum verhindern und wenn, dann nur mit teuren Zusatztools. Daher sind solche Geräte immer ein potentielles Einfallstor für Viren. Es ist also extrem wichtig, dass Sie dafür sorgen, dass auf den Geräten ein Virenscanner installiert ist und ein internes Verwaltungsprogramm im Einsatz ist, das die Endgeräte überwacht und Viren gegebenenfalls entfernen kann.

Windows Phone ist genauso restriktiv wie iOS und daher gut geeignet für den Unternehmenseinsatz. Mit dem neuen Microsoft System Center 2012 lassen sich Windows Phone-Geräte darüber hinaus gut verwalten. Natürlich unterstützen Windows Phone-Geräte auch die Microsoft Exchange ActiveSync-Richtlinien und das Fernlöschen über Exchange. Seine Stärken spielt Windows Phone bei der Anbindung an Exchange und SharePoint aus. Durch das integrierte Office-Mobile können Anwender ohne die Installation von Apps schnell und einfach auf Exchange und SharePoint zugreifen, auch über das Internet. Durch Outlook Mobile lassen sich Besprechungsanfragen von Exchange noch besser nutzen als in den Konkurrenzsystemen. Windows Phone ermöglicht keinen Anschluss von Speicherkarten wie SD. Das erschwert den Datenaustausch, erhöht aber den Datenschutz.

SharePoint Workspace Mobile

Der Austausch von Dokumenten mit Windows Phone 7.5 erfolgt am besten über das Senden per E-Mail oder dem Speichern in SharePoint. Auch SharePoint Workspace Mobile ist direkt in Windows Phone integriert, Sie müssen keine App herunterladen und nichts lizenzieren. Der Zugriff auf die Dokumente kann dann auch durch Office Web Apps erfolgen, also ebenfalls wieder kostenlos online oder über SharePoint, wenn Sie Office Web Apps in Ihrer SharePoint-Farm installiert haben. Sie können dazu SharePoint im Internet veröffentlichen, zum Beispiel über das TMG 2012 oder UAG 2012 oder auch auf anderem Weg.

SharePoint Workspace Mobile zeigt auch Dokumente an, die Anwender bereits über SharePoint geöffnet haben. Die Dokumente stehen auch offline zur Verfügung, das heißt, wenn kein Zugriff auf SharePoint besteht. Um eine SharePoint-Seite zu öffnen, geben Sie auf der Seite "URL öffnen" einfach die Adresse ein. Anschließend bindet SharePoint das Windows Phone an. Sind für die Seite noch Authentifizierungsdaten notwendig, erscheint ein weiteres Fenster, in dem Benutzer den Benutzernamen, die Domäne und das Kennwort eingeben müssen. Nach der erfolgreichen Authentifizierung öffnet sich die Anzeige der SharePoint-Seite mit allen Dokumenten, Listen, Bibliotheken und weiteren Inhalten. Die Seiten sind dazu speziell für Windows Phone angepasst. Die Anbindung ist auch problemlos mit Small Business Server 2011 Standard beziehungsweise SharePoint Foundation 2010 möglich.

Sollen mobile Anwender über das Internet auf SharePoint zugreifen, ist es notwendig, die Dienste zu veröffentlichen oder ein VPN zu verwenden. Neben dem Forefront Threat Management Gateway 2010 (TMG) bietet Microsoft noch das Forefront Unified Access Gateway 2010 (UAG) an. Hierbei handelt es sich um eine erweiterte Version des TMG, die besser für SharePoint geeignet ist. Der Vorteil der größeren UAG-Version ist die Unterstützung von AAM (Alternative Access Mappings, alternative Zugriffszuordnungen). Mit dieser Funktion können Sie URLs zu SharePoint frei definieren und zu den internen Webanwendungen umleiten. Zusätzlich unterstützt das UAG die Webanwendungen von SharePoint und bindet diese in die Veröffentlichung ein.

SharePoint 2010 und das iPhone

Sie können mit iPhones auch auf Daten von SharePoint 2010-Servern zugreifen. Es gibt mehrere Apps, die SharePoint unterstützen. Ein bekanntes und kostenloses App ist "Moshare", das auch die Anbin-

Bild 2: Mit "SharePoint Workspace Mobile" greifen auch mobile Geräte mit kleinen Displays komfortabel auf SharePoint zu

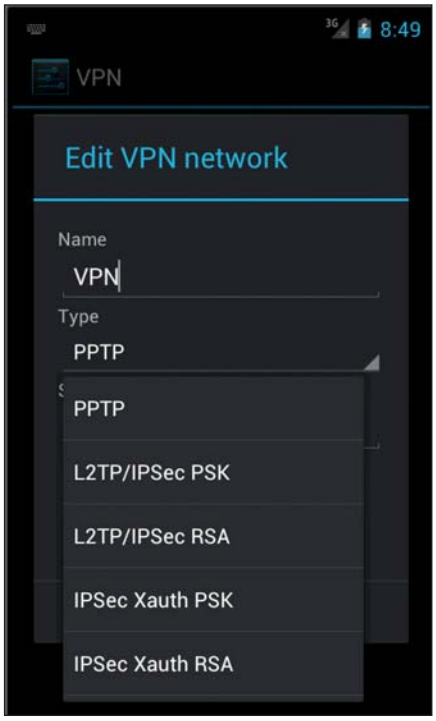


Bild 3: Unter Android lassen sich VPNs mit verschiedenen Authentifizierungsmechanismen einrichten

dung an SharePoint 2010 problemlos unterstützt. Vor allem die Anzeige von Kalendern ist über das App besser gelöst als der Zugriff über den Safari-Browser. Moshare eignet sich allerdings, wie die anderen kostenlosen Apps, nur für den lesenden Zugriff auf Word-, PowerPoint-, Excel-, PDF-, Text-Dokumente sowie Bilder. Visio-Zeichnungen oder InfoPath-Formulare können Sie nicht lesen. Für den Zugriff auf Browser-integrierte InfoPath-Formulare verwenden Sie Safari, wobei jedoch nicht alle funktionieren. Moshare kann problemlos über das Internet auf SharePoint zugreifen, allerdings müssen Sie dazu die SharePoint-Site im Internet veröffentlichen oder per VPN zugreifbar machen.

Eine weitere kostenlose App, um das iPhone mit SharePoint zu verbinden, ist "SharePlus Lite Office Mobile Client". Diese App – wie auch Moshare – finden Sie im App-Store zum kostenlosen Download. Es spricht generell nichts dagegen, mehrere Apps zu testen, da sich die Konfigurationen und der Betrieb der Apps gegenseitig nicht stören. Die Bedienung beider Apps ist sehr einfach und auch das Bewegen durch die SharePoint-Daten ist kein größeres Problem. Geübte Anwender kommen schnell damit zurecht. Sie können in Moshare auch mehrere verschiedene SharePoint-Websites einbinden, auch mit verschiedenen Anmeldedaten. Auf diese Weise ist es möglich, sich mit wenigen Klicks erst mit einem Benutzerkonto und dann als Administrator einzuloggen. Rufen Sie eine Bibliothek auf, sehen Sie alle enthaltenen Dokumente.

Mit "SharePlus Lite Office Mobile Client" gehen Sie ähnlich vor. Auch hier müssen Sie zuerst die Daten für die Anmeldung eingeben und können dann in der App mit Ihren Benutzerinformationen in SharePoint Daten abrufen. Das Lesen von Dokumenten ist mit dieser App ebenfalls problemlos möglich. SharePlus Lite Office Mobile Client unterstützt, neben der standardmäßige Windows-Authentifizierung, auch die formularbasierte Authentifizierung in SharePoint 2010. Auch die App "iShare" ist kostenlos, aber mittlerweile veraltet und nicht kompatibel mit iOS4 und vor allem nicht mit SharePoint 2010. Weitere Apps, die allerdings kostenpflichtig sind, finden Sie über PocketPoint, SharePlus Office Mobile Client, iSP-Browser und Attaché SharePoint Client.

VPN mit iPhone

Neben der Möglichkeit, auf Exchange oder SharePoint zuzugreifen, lassen sich Smartphones auch per VPN anbinden. Installierte Apps können dann über Netzwerkverbindungen auf Daten im Unternehmen zugreifen. Bei der Anbindung an ein VPN verhalten sich iPhones wie ein normaler PC. Das heißt im Unternehmen benötigen Sie einen ganz normalen VPN-Zugang, kein besonderes Endgerät. Das kann ein VPN-Router sein oder ein Windows-Server – beziehungsweise ein TMG / ISA / USAG. Die Anbindung erfolgt über interne Einstellungen auf dem iPhone.

Für Hersteller wie Juniper oder Cisco stehen im Appstore Apps zur Anbindung bereit, die die Konfiguration und den Start des VPNs vereinfachen und den Datenverkehr steuern. Als Protokolle unterstützt das iPhone L2TP/IPSec, PPTP und Cisco IPSec. Das heißt, Sie können jeden VPN-Server einsetzen, der diese Protokolle unterstützt. Die Benutzerauthentifizierung realisieren Sie über MS-ChapV2, RSA SecurID mit CryptoCard oder über einen symmetrischen Schlüssel (Shared Secret). Der Client für Cisco steht als App im Appstore zur Verfügung. Die Software verwendet SSL (Secure Sockets Layer) und DTLS (Datagram Transport Layer Security). Der Client unterstützt die manuelle Konfiguration, aber auch den Import von Profilen mit dem iPhone-Konfigurationsprogramm.

VPN mit Android-Clients

Wollen Sie vernünftig mit VPNs arbeiten und sogar zusätzliche Apps für den Verbindungsaufbau nutzen, müssen Sie in vielen Fällen das Android rooten, da die meisten VPN-Apps erweiterte Rechte benötigen und die Standardrechte des Benutzers nicht ausreichen. Standardmäßig unterstützt Android PPTP mit Shared Secret, L2TP und L2TP/IPSec entweder mit Zertifikat oder Shared Secret. Mit Android 2.1/2.2/2.3 lassen sich zwar auch viele VPNs über den integrierten Standard-Client einrichten, aber längst nicht alle. Die Versionen sind zwar veraltet, aktuell ist derzeit 4.0.4, aber trotzdem noch sehr häufig im Einsatz. Für viele VPNs benötigen Sie keine VPN-App, sondern können den internen Client in Android verwenden.

Arbeiten Sie mit einem zertifikatgesicherten VPN, müssen Sie vor dem Verbindungsaufbau das Zertifikat auf die SD-Karte des

Bild 4: Moshare bringt die Dokumente einer SharePoint-Bibliothek auf das Smartphone

Android kopieren und es installieren. Haben Sie eine Zertifikate-Datei auf das Android kopiert, installieren Sie das Zertifikat über "Einstellungen \ Standort und Sicherheit \ Von SD-Karte installieren".

Unternehmen, die OpenVPN einsetzen, können Android-Handys per VPN verbinden, indem sie die App OpenVPN aus dem Market auf den Endgeräten installieren. OpenVPN baut auf SSL auf und ist bezüglich der Konfiguration sehr flexibel. Die Authentifizierung kann über Zertifikate oder über Shared Secret erfolgen. Die Verbindungsdaten geben Sie dann im Client auf dem Handy ein. Damit Sie die App OpenVPN GUI (Root) verwenden können, benötigen Sie Root-Rechte auf dem Telefon. Eine weitere App, welche die Einstellung von OpenVPN auf dem Android vereinfacht, ist "OpenVPN Settings". Auch diese App benötigt Root-Rechte.

Arbeiten Sie mit speziellen Geräten wie zum Beispiel SonicWALL oder Cisco, ist natürlich nicht immer ein spezieller Client notwendig. Sie können in den meisten Fällen auch mit den Standardeinstellungen in Android arbeiten, wenn der VPN-Server entsprechend konfiguriert ist. Verwenden Sie zum Beispiel ein VPN mit der Einstellung L2TP/IPSec PSK-VPN auf dem Android, deaktivieren Sie die Option "L2TP-Schlüssel aktivieren" in den Einstellungen, wenn die Verbindung nicht funktioniert.

Wer Android-Handys mit Exchange verbinden will, findet im Market auch verschiedene, teilweise kostenlose Apps, die viele Probleme beheben, die die Standard-Anwendung in älteren Android-Versionen hat. "Nitrodesk TouchDown" gibt es als 30-Tage-Testversion im Market. Allerdings läuft die App nicht auf allen Android-Handys. Damit lassen sich mehr Einstellungen vorgeben und auch Aufgaben synchronisieren. Eine weitere interessante Anwendung ist "Enhanced Email". Auch hier lassen sich verschiedene Einstellungen ändern sowie Ports und Zertifikate besser verwalten. "Corporate Addressbook" ermöglicht einen besseren Zugriff auf die globale Adressliste (GAL) von Exchange, "Out of Office Assistant" kann den Abwesenheitsassistenten über das Android steuern. Viele Hersteller, zum Beispiel HTC, bauen eigene Anwendungen für die Exchange-Anbindung ein, die wesentlich besser funktioniere als die Standard-App. Wollen Sie zum Beispiel Besprechungsanfragen beantworten, kann das die Standard-App nicht optimal. HTC-Androids arbeiten hier etwas besser, aber auch nicht perfekt.

Zusatzanwendungen für Exchange-Anbindung

Android sicher an Unternehmen anbinden

Um Android 4-Geräte sicher anzubinden, kommen IT-Verantwortliche um eine Zusatzsicherheitslösung kaum herum. Bekannt in diesem Bereich ist MobileIron. Das Unternehmen bietet eine Sicherheitssuite für Android-Geräte. So ermöglicht das Werkzeug beispielsweise die Verschlüsselung der Daten, eine VPN-Verbindung über Cisco AnyConnect und zentrale Verwaltung des Clients, erlaubt Exchange-Konten zu konfigurieren (inklusive der Zertifikate) und das Sperren von Geräten unter Einsatz von Richtlinien. Vor allem bei der Anbindung zahlreicher Android-Geräte an Unternehmensnetzwerke ist der Einsatz solcher Lösungen empfehlenswert, die mittlerweile von zahlreichen Herstellern angeboten werden.

Mit McAfee Enterprise Mobility Management (EMM) können Sie Richtlinien auch gruppenbasiert im Active Directory umsetzen, Einstellungen automatisieren, die Endgeräte vor Viren schützen und angebundene Geräte überwachen sowie Apps automatisiert installieren lassen. Die Software ist kompatibel zu iPhones, Android, HP WebOS und Windows Mobile, Blackberry und Windows Phone 7/7.5. Die McAfee-Infrastruktur besteht aus einem oder mehreren Servern. Mit der E-Mail-Proxy-Server-Funktion stellen Sie in der DMZ einen Proxy-Server zur Verfügung, der die Exchange ActiveSync-Anfragen sicher zwischen Internet und internem Netzwerk routen kann.

McAfee EMM kann im Gegensatz zu Exchange-Remote-Wipe aber zwischen den Daten auf den Endgeräten unterscheiden. Setzen Sie Exchange ein, um Daten remote zu löschen, dann setzt Exchange immer das komplette Gerät mit allen Daten zurück. Das ist beim Einsatz von privaten Smartphones problematisch, da auch die privaten Daten der Anwender verlorengehen. EMM kann auch partiell einzelne Daten zurücksetzen, zum Beispiel E-Mails, Kontakte oder den Kalender. Ebenfalls über die Einstellungen in der Richtlinie

Bild 5: Haben Unternehmen bereits eine Sicherheitslösung im Haus, so bietet diese oft eigene Clients für mobile Geräte, wie beispielsweise der Cisco-VPN-Client

funktioniert das Sperren von Gerätefunktionen und das Hinterlegen von VPN-Einstellungen oder WLAN-Verbindungen.

Sybase Afaria, eine Tochter von SAP, bietet mit "Sybase Afaria Advanced Enterprise Security (AES) for Android" ein Produkt, das Android zentral verwalten kann. Apps lassen sich remote installieren, entfernen, blockieren und überprüfen. Über Richtlinien lassen sich Einstellungen vorgeben und Funktionen sperren. Geräte und Daten lassen sich löschen, auch auf SD-Karten. Sybase ist vor allem auf Android spezialisiert. Es gibt aber auch Versionen für iOS 4 und 5.

Auch "Zenprise MobileManager" geht in die gleiche Richtung. Hier lassen sich Geräte zentral verwalten und sogar für den Zugriff auf das interne Netzwerk sperren. Besonderheiten sind ein eigener Appstore und eine Unterscheidung zwischen privaten und beruflichen Daten. Die Unternehmensdaten speichert Zenprise an einem gesicherten Ort auf den Smartphones. *(jp)*

[1] Kostenloses iPhone-Konfigurations-Programm B9P21

Link-Codes

Datensicherheit mit dem Trusted Platform Module

Kleiner Chip, große Wirkung

von Dr. Holger Reibold

Quelle: philhol - 123RF

Mit der rasanten Verbreitung mobiler Geräte wächst auch die Notwendigkeit, die Kommunikation von und mit derlei Geräten sicherer zu gestalten. Neben verschiedenen softwarebasierten Lösungen soll insbesondere ein neues Hardware-Element den gestiegenen Sicherheitsanforderungen einer modernen Infrastruktur Rechnung tragen: das Trusted Platform Module, kurz TPM. IT-Administrator zeigt, wie praxistauglich die Technik ist und wie Sie die ersten Gehversuche damit unternehmen.

In der Trusted Computing Group (TCG) verfolgt niemand geringeres als Branchengrößen wie AMD, Hewlett-Packard, IBM, Infineon, Intel, Lenovo, Microsoft oder Sun die Entwicklung einer vertrauenswürdigen Plattform. Geht es nach dem Willen der TCG, werden in Zukunft in Mobilgeräten, Notebooks, Desktop-PCs und Server entsprechende Komponenten verbaut, die die Sicherheit auf ein neues Level heben sollen. Implementiert ist die vertrauenswürdige Plattform in einem Chip, der sich ähnlich wie eine Smartcard verhält, aber statt an einen spezifischen Benutzer an eine Hardware-Instanz geknüpft ist.

Bezeichnet wird ein Gerät, das mit einem TPM sowie einem TPM-fähigen Betriebssystem und einer entsprechenden Software ausgestattet ist, als "Trusted Computing Platform". Es sollen dadurch keine Datenänderungen oder -Nutzungen gegen den Willen des Eigentümers möglich sein – vorausgesetzt, dieser hat entsprechende Beschränkungen eingerichtet. Das TPM und seine Implementierung kennzeichnen außerdem, dass dieses überwiegend passiv zum Einsatz kommt und einen eindeutigen kryptografischen Schlüssel besitzt, der beispielsweise zur Identifizierung eines Rechners verwendet werden kann. Voraussetzung hierfür ist allerdings, dass das Auslesen dieser Informationen aktiviert wurde.

Vorteile von TPM

Bei einem TPM-fähigen Gerät bestimmt der einzelne Anwender über die Chip-Konfiguration, ob und falls ja, welche TPM-Funktionen zum Einsatz kommen. Er kann das TPM-fähige Gerät zunächst als sicheren Speicherort für seine Schlüssel verwenden. Mithilfe dieser Schlüssel lassen sich die Daten auf dem Gerät durch den Eigentümer oder Geräteadministrator verschlüsseln. Auch das Signieren von Dateien unterstützt TPM. All diese Funktionen sind zunächst auch von Smartcards bekannt. Doch TPM geht noch einen Schritt weiter und beinhaltet Security Policies, die festlegen, welche Daten des Geräts wie verwendet werden dürfen. So lassen sich beispielsweise Bearbeitungs-, Kopier- oder Versandberechtigungen benutzer- und gruppenspezifisch anlegen und verwalten. Damit ein Benutzer – es kann sich dabei auch um eine externe Applikation handeln – bestimmte Aktionen auf dem System ausführen kann, muss es diesem gegenüber ein gewisses Vertrauen entgegenbringen.

Um Security Policies auch im kommerziellen Umfeld anwenden zu können, bedarf es eines Kontrollmechanismus, der sicherstellt, dass die definierten Richtlinien auch eingehalten werden. Genau dies ist die Aufgabe von TPM. Die Richtlinien stellen zudem sicher, dass die Vorgaben von externen Usern auf dem TPM-fähigen Gerät nicht umgangen werden können. Ein Nutzer A könnte beispielsweise für seine Daten auf dem TPM-Gerät des Nutzers B bestimmte Regeln anlegen. Kann B nun A belegen, dass diese Sicherheit gewährleistet ist, handelt es sich um ein sogenanntes Trusted System.

Die nächste Frage ist, wie eine Sicherung von eigenen Daten auf einem Fremdsystem ohne Eingriffe in die Systemkonfiguration möglich ist. Das ist nämlich bei keinem klassischen Betriebssystem – und zwar unabhängig von dessen Flexibilität in Sachen Sicherheitskonfiguration – möglich. Die Lösung: Die Hardware-basierte Implementierung der Sicherheitsfunktionen im TPM. Das Modul wird fest

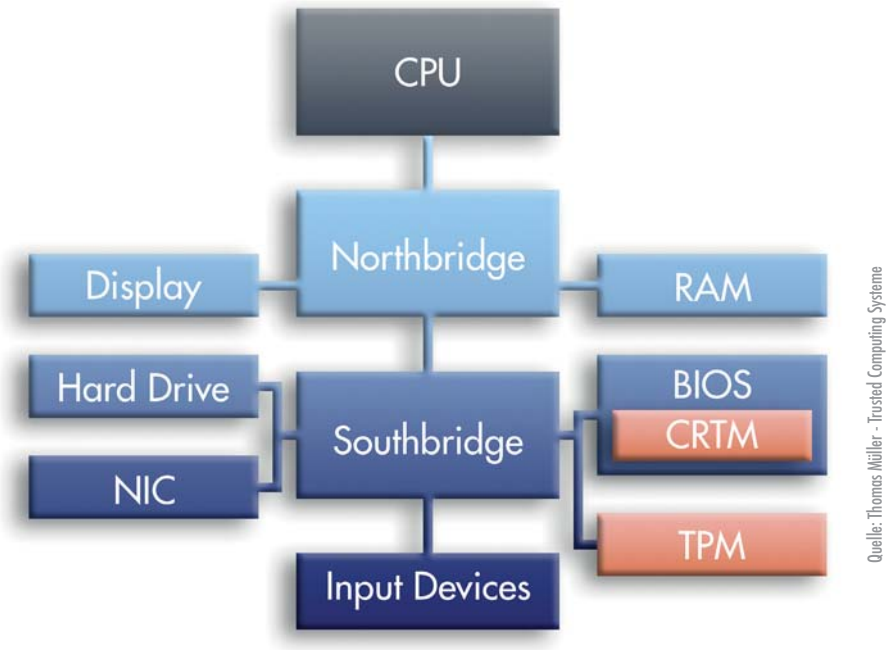


Bild 1: So könnte eine Referenzarchitektur mit einem TPM-Element auf einem Mainboard aussehen

mit der verwendeten Hardware verknüpft oder kann auch vollständig in zu verwendenden Chip-Sätzen integriert sein. Die enge Verknüpfung der klassischen Hardware mit dem TPM-Modul verspricht somit ein hohes Maß an Sicherheit.

Das TPM besitzt eine eindeutige ID, die es nach außen kommunizieren, aber auch gleichzeitig vor neugierigen Blicken verbergen kann. Ist auf einem Rechner die TPM-Unterstützung aktiv, übernimmt der Sicherungsmechanismus die Rolle des Auditors. Der Eigentümer des TPM-Gerätes kann zwar die TPM-Unterstützung deaktivieren, hat aber selbst keine Zugriffsmöglichkeiten auf gesicherte Daten – ein grundlegender Unterschied gegenüber klassischen Server-Plattformen, bei denen der Administrator immer vollständigen Zugriff auf alle Daten und Einstellungen hat.

Schwachstelle Betriebssystem

TPM nutzt öffentliche Schlüssel als Teil seiner ID. Ein externer User kann damit die Daten auf einem TPM-gesicherten Gerät so verschlüsseln, dass diese nur mit einem privaten Schlüssel wieder entschlüsselt werden können. Das Interessante dabei: Der externe User kann Bedingungen definieren, die erfüllt sein müssen, bevor sich die Daten überhaupt mit dem privaten Schlüssel entschlüsseln lassen. Die auf dem Modul abgelegten Schlüssel werden wiederum mit dem sogenannten Storage Root Key, kurz SRK, geschützt. Dabei handelt es sich um einen RSA-Schlüssel mit einer Länge von 2.048 Bit. Die Bezeichnung rührt daher, dass es sich um den Wurzelschlüssel des TPM-Schlüsselbaums handelt. Wechselt der Eigentümer eines Rechners, wird auch ein neuer SRK generiert.

Auch der Besitzer eines TPM-Geräts kann natürlich seine Daten mit Zugriffsbedingungen schützen. Dieser Vorgang wird als Sealing (Versiegelung) bezeichnet. Dabei werden die betreffenden Daten an ein spezifisches TPM gebunden. Die Verknüpfung von Zugriffsbedingungen und Verschlüsselungstechniken heißt Binding. An dieser Stelle zeigt sich ein Knackpunkt von TPM: Das verwendete Betriebssystem muss sicherstellen können, dass die Daten nicht manipulierbar sind. Doch weder Mac OS X noch Linux oder Windows bieten in den aktuell verfügbaren Versionen eine entsprechende Unterstützung der TPM-Funktionalität.

Zwei weitere Techniken bedürfen der näheren Betrachtung: Wie kann die Identitätsprüfung eines TPMs erfolgen und wie lässt sich herausfinden, welche Prozesse auf einem TPM-Gerät verfügbar sind? Damit ein externer Benutzer seine kritischen Daten mittels TPM überhaupt sichern kann, müsste er das betreffende Modul zunächst als solches identifizieren. Dazu bedient sich der TPM-Mechanismus des sogenannten Endorsement-Zertifikats. Mit diesem Schlüssel bescheinigt ein Hersteller einer TPM-Einheit, dass das Gerät und der zugehörige öffentliche Schlüssel den TCG-Spezifikationen entsprechen. Ein externer User kann einen Request an das Gerät schicken – genauer gesagt: eine Zufallszahl –, die dann vom TPM-Gerät mit dem zum öffentlichen Schlüssel passenden privaten Schlüsseln kodiert wird. Anhand der Rückgabe des Challenge-Response-Verfahrens kann der externe User sicherstellen, dass es sich bei dem angefragten Gerät um eine funktionstüchtige TPM-Einheit handelt. Für die Ausstellung der Zertifikate wird eine entsprechende unabhängige Certificate Authority benötigt.

Um die Verfügbarkeit bestimmter TPM-Funktionalität eines Systems abrufen zu können, verwendet der Sicherungsmechanismus das sogenannte Platform Configuration Register. Darin sind verschiedene Spezifika des TPM-Geräts hinterlegt. Nur wenn die angeforderten und bereitgestellten Funktionen übereinstimmen, kann ein externer User das TPM-System verwenden.

Zertifikate für Vertraulichkeit

Die Entwickler von TPM mussten bei ihrem Entwurf der vertrauenswürdigen Plattform einerseits die geänderten Anforderungen in Sachen Sicherheit, andererseits auch die Erweiterbarkeit bestehender Hardware berücksichtigen. Da Software per se immer sicherheitsanfällig ist, war die Lösung offensichtlich: Das Implementieren des TPM-Sicherheitsmechanismus in einen externen Prozessor. Doch das alleine würde nicht genügen, um TPM nutzen zu können. Die TPM-Spezifikationen sehen neben dem Hardware-basierten Sicherungsmechanismus verschiedene Hilfsmodule vor, die zum einen die BIOS-Funktionalität erweitern, zum anderen Steuerungsaufgaben übernehmen. Das Zusammenspiel dieser Komponenten soll sicherstellen, dass ein Computer einen für Dritte vertrauenswürdigen Zustand besitzt und diesen auch nachweisen kann.

Die Kernfunktion von TPM ist das Sicherstellen der Vertraulichkeit. Dabei

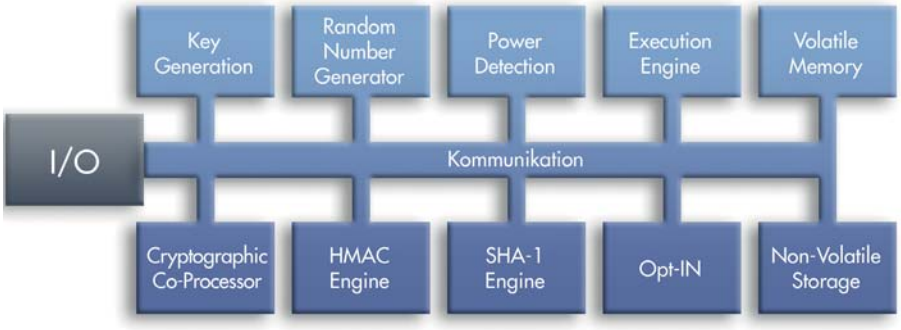


Bild 2: Die Komponenten der TPM-Architektur

kommen verschiedene Zertifikate zum Einsatz, mit denen die Authentizität und Integrität der Systeme gewährleistet wird. Das Endorsement-Zertifikat bescheinigt die Echtheit eines TPM. Es bestätigt, dass das TPM von einem autorisierten Hersteller stammt. Das Zertifikat besteht aus einem 2.048 Bit langen Schlüsselpaar und ist fest an diesen Chip geknüpft. Der Endorsement Key dient außerdem zum Erzeugen eines sogenannten Attestation Identity Key, einer Art Alias für das TPM. Das Plattformzertifikat, mit dem der Gerätehersteller einen PC, Notebook oder Smartphone ausstattet, dient als Nachweis, dass das Gerät die Anforderungen der TCG-Spezifikation erfüllt. Damit ist sichergestellt, dass es sich um ein prinzipiell vertrauenswürdiges System handelt und es entsprechend genutzt werden kann.

Die TPM-Plattform verwendet zwei weitere Zertifikate: Mit dem sogenannten Conformance-Zertifikat wird bestätigt, dass das Gerätedesign der Spezifikation entspricht, und mit dem Validation-Zertifikat ist sichergestellt, dass es entsprechend den offiziellen Vorgaben implementiert ist. Alle vier Zertifikate sind fest in das TPM-Gerät integriert und befinden sich an vorgegebenen Speicherplätzen, damit sie gegebenenfalls von außen (auch vom verwendeten Betriebssystem des TPM-Geräts) angesprochen und abgefragt werden können.

Da das TPM per Definition ein passives Modul ist, erfolgt die Abfrage immer von außen. Hierfür sieht die TCG-Spezifikation eine spezielle Schnittstelle vor, die die Kommunikation mit dem verwendeten Mainboard erlaubt. Dank der Kapselung, die das TPM-Modul von der Hauptplatine und der aufsetzenden Software trennt, ist die TPM-Einheit per Software nicht manipulierbar.

Mögliche Anwendungsszenarien

Es gibt verschiedene Szenarien, in denen der Einsatz der TPM-Mechanismen besonders sinnvoll erscheint. Das wichtigste Ziel von TPM wurde bereits genannt: Das Sicherstellen der Integrität eines Systems. Damit ist vor allem gemeint, dass sich dieses wie beabsichtigt verhält und keine abnormen Verhaltensweisen zeigt. Die Vertrauenswürdigkeit ist dabei nicht nur auf einen Desktop-PC oder das aufsetzende Betriebssystem beschränkt, sondern schließt auch den Boot-Vorgang, die System- und Anwendungsausführung ein. Im Zusammenspiel mit dem BIOS formt TPM die sogenannte Root of Trust. Das TPM beinhaltet verschiedene Platform Configuration Register, in denen die verschiedenen sicherheitsrelevanten Metriken hinterlegt werden. Diese Informationen werden genutzt, um Änderungen der Systemkonfiguration zu erkennen und um gegebenenfalls Folgemaßnahmen einzuleiten.

Anwendungen, die der Festplattenverschlüsselung dienen wie Microsofts BitLocker, können das TPM nutzen, um die Schlüssel zu schützen, die für die Festplattenverschlüsselung verwendet werden. Ein weiterer Anwendungsbereich ist der Passwortschutz. Der Zugriff auf Schlüssel, Daten und Computersysteme wird oftmals durch ein klassisches Passwort geschützt. Die Authentifizierung erfolgt dabei typischerweise rein auf Software-Basis und ist daher für Passwort-Attacken anfällig. Der TPM-Mechanismus verfügt über einen speziellen Hardware-Schutz, der Wörterbuchabfragen erkennt.

Prinzipiell kann jede Anwendung, die ein bestimmtes Maß an Sicherheit verlangt, TPM nutzen. Denkbare Einsatzbereiche sind beispielsweise das Digital Rights Management, aber auch der Schutz von Software-Lizenzen. Sinnvoll erscheint die TPM-Nutzung prinzipiell überall dort, wo ein hohes Maß an Vertraulichkeit gefragt ist. Das ist beim "einfachen" Online-Shopping oder -Banking genauso der Fall wie bei aufwendigen B2B-Transaktionen.

Noch nicht praxistauglich

Die ersten Entwicklungen in Sachen Trusted Platform Module sind schon über eine Dekade alt, doch noch sind wir weit entfernt von einer breiten Nutzung dieser Technik. Gründe hierfür gibt es verschiedene: Die Technik ist immer noch den Beweis schuldig, ob sie die Anforderungen in der Praxis erfüllen kann. Bislang fehlt es an Erfahrungen, die belegen könnten, dass TPM die gewünschte Vertraulichkeit auch tatsächlich gewährleistet.

Theoretisch kann TPM jedes beliebige Computer-System in eine vertrauenswürdige Plattform für externe Benutzer verwandeln – doch noch scheiden sich die Geister daran, ob die hohen Erwartungen

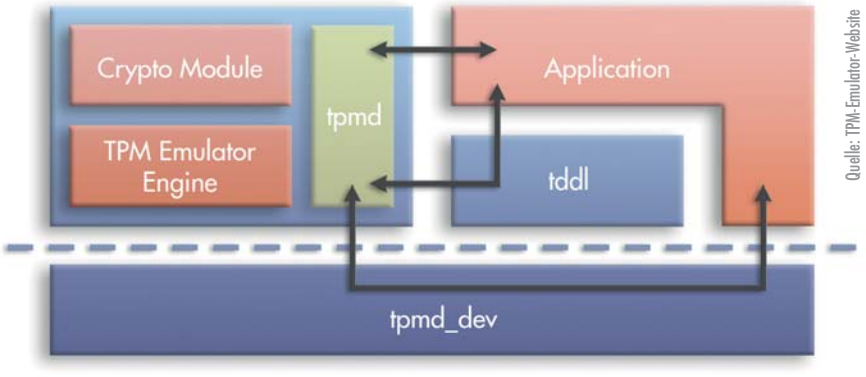


Bild 3: Das Design des TPM-Emulators erlaubt das lokale Testen der TPM-Funktionalität

auch erfüllt werden können. In der Vergangenheit war immer wieder festzustellen, dass die Befürworter dieser Technik dank ihrer exponierten Marktposition TPM insbesondere mit eigenen DRM-Techniken und eigenen Lösungen in den Medien lancieren.

Zwar sind die Spezifikationen der TCG für jedermann öffentlich zugänglich, kleinere und mittlere Entwickler bleiben allerdings bei der Ausgestaltung des Standards aufgrund der hohen Mitgliedsbeiträge außen vor. Dass die TCG und insbesondere deren Führung ausnahmslos von Vertretern der Großen in der IT-Branche dominiert werden, hat in der Vergangenheit immer wieder den Unmut von interessierten Entwicklern geschürt.

Das TPM ist durch den vertrauenswürdigen Systemstart, den Schutz von Daten auf eigenen und Fremdsystemen sowie die Beglaubigung der Plattform durch Dritte gekennzeichnet. Als problematisch wird allerdings von vielen die Tatsache empfunden, dass die Vertraulichkeit des eigenen Systems beziehungsweise einer zentralen Sicherheitskomponente durch eine externe Beglaubigungsstelle bestätigt wird. Viele Anwender befürchten Einschränkungen bei der Nutzung und Kontrolle der eigenen Hard- und Software. Ausgesprochen kontraproduktiv für eine breite Akzeptanz von TPM wirkt ein weiterer Umstand: Viele freie Entwickler scheuen ein Engagement in Sachen TPM, weil sie nicht abschätzen können, ob sie womöglich mit Lizenz- oder Patent-Ansprüchen konfrontiert werden. Solche Bedenken bedeuten oftmals den Todesstoß für freie Projekte oder ersticken erste Überlegungen in dieser Hinsicht schon im Keim.

Als ein weiteres Hindernis könnte sich die Bindung von Software und Inhalten an eine Hardware-Komponente erweisen. Kommen nicht-migrierbare Schlüssel zum Einsatz, so sind die Inhalte an diese Komponente geknüpft. Eine praktikable Lösung für dieses Problem bietet die TCG-Spezifikation bislang nicht. Bei der Diskussion um TPM werden auch immer wieder Stimmen laut, die Sinn und Zweck dieser Sicherungstechnik generell in Zweifel ziehen, denn TPM ähnelt der Smartcard-Technik sehr. Kritiker erachten die Verknüpfung von Daten mit Benutzern für sinnvoller als die Bindung an eine spezifische Plattform.

Die erste Anlaufstelle für Informationen rund um TPM ist die Website der Trusted Computing Group. Unter [2] finden Sie die aktuellen Spezifikationen sowie einen Überblick über aktuell verfügbare Entwicklerwerkzeuge und weitere nützliche Informationsquellen.

Trusted Computing Group

Erfahrungen mit dem TPM-Emulator sammeln

Zwar sind inzwischen viele Business-PCs mit einem TPM-Chip ausgestattet oder können mit einem entsprechenden Steckmodul einfach erweitert werden, doch wie sammeln Sie in der Praxis am besten Erfahrungen mit dieser Technik? Heiko Stamer und Mario Strasser haben mit dem TPM-Emulator [1] einen Open Source-Emulator für Linux entworfen, der die Funktionen des TPM-Chips nachstellt. In dem Emulator wurden rund 100 der 120 durch die TCG in der Spezifikation "TPM Main Part 3 Commands" beschriebenen Funktionen implementiert. Um den TPM-Emulator zu starten, verwenden Sie folgende Anweisung:

```
tpmd -u /Socket-Verzeichnis/Socket-
  Datei -s /Storage-Verzeichnis/Sto-
  rage-Datei -d -f clear
```

Wichtig ist dabei, dass das Socket- und Storage-Verzeichnis bereits angelegt sind. Die Socket-Datei darf zum Zeitpunkt des Starts des Emulators nicht existieren. Die Socket-Datei sorgt für die Verbindung zwischen dem TPM-Emulator und den Anwendungen und ermöglicht somit den Datenaustausch. Wichtig ist außerdem, dass Sie beim ersten Start des TPM-Emulators den Startup-Modus "clear" verwenden.

Bei TPM handelt es sich um ein zeichenorientiertes Gerät (Character Device), das unter Linux mit der Major-Nummer 10 und der Minor-Nummer 224 registriert ist. Daher muss auch der TPM-Emulator mit diesen Werten in Linux eingerichtet werden. Dazu verwenden Sie folgenden Befehl:

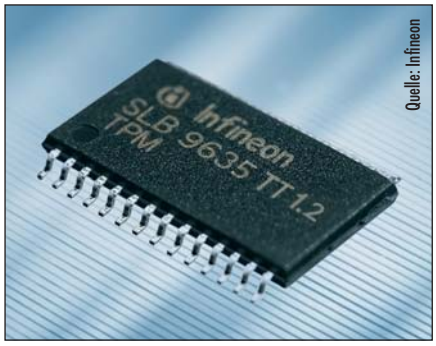


Bild 4: Mit entsprechender Software bieten Chip-Hersteller wie Infineon auf Windows abgestimmte TPM-Sicherheitslösungen

```
# mknod /dev/tpm c 10 224
```

Um die Verbindung zwischen Gastsytem und TPM-Emulator herzustellen, verwenden Sie folgende Kommandos:

```
# modprobe tpm_atmel
# tcsd
```

Mithilfe der TPM-Tools können Sie nun direkt Befehle an den TPM-Emulator senden. Die Tools stellen eine begrenzte Anzahl des TPM-Befehlssatzes für die Konsoleneingabe zur Verfügung. Um die Version des TPMs abzurufen, verwenden Sie beispielsweise den Befehl *tpm_version*.

Fazit

Mit TPM steht eine überaus interessante Technik zur Verfügung, mit der Benutzer ihre Daten sicher auf Drittsystemen ablegen und gegebenenfalls mit Dritten teilen können. Dabei ist aber auch die notwendige Vertrauenswürdigkeit sichergestellt, dass die Daten nicht manipuliert werden können – nicht einmal vom Betreiber des Systems. Benutzer können Daten zudem sicher auf externen Computer speichern und dabei die Bedingungen für die Datennutzung vollständig selbst bestimmen. Das macht TPM besonders interessant, gerade auch angesichts der rasanten Zunahme der Nutzung von Cloud- und Web-basierten Services. *(dr)*

[1] TPM-Emulator
C7P51

[2] Trusted Computing Group
C7P52

Link-Codes

Sicherheit unter Windows 8

Festung Windows

von Thomas Gronenwald

Mit der Veröffentlichung von Windows 7 hat Microsoft bereits einiges für die Sicherheit des Betriebssystems getan. In Windows 8 bauen die Redmonder ihr Sicherheitskonzept weiter aus und wollen so den Schutz vor Angriffen erhöhen. Ein integrierter vollwertiger Virenschutz, ein eigener PDF-Reader und ein Reset-Knopf für das Betriebssystem sind nur drei Beispiele. Für die Anwender dürfte es zumindest einfacher werden, ihren Rechner sicher zu betreiben. Und auch den Trend zu "Bring Your Own Device" hat Microsoft im Blick.

Nur noch in vier Versionen will Microsoft das neue Windows 8 veröffentlichen. Neben einer Standardversion (Windows 8) soll es die erweiterte Ausführung Windows 8 Pro für den professionellen Einsatz sowie mit Windows 8 Enterprise eine Variante für den Einsatz im Unternehmen geben. Die Enterprise-Version adressiert die Bedürfnisse in Unternehmen und enthält neben den standardmäßigen Features aus der Standardversion zahlreiche weitere interessante Features aus den Bereichen Virtualisierung, Deployment, Security und Management. Windows 8 Enterprise bleibt allerdings nur Unternehmen mit einem gültigen Volumenlizenzvertrag vorbehalten. Für den Einsatz auf Tablets mit ARM-Prozessoren will der Software-Anbieter zudem eine spezielle Variante anbieten.

Verbesserter Virenschutz

Microsoft spendiert seinem neuen Betriebssystem einen nahezu vollständig in das Betriebssystem integrierten Virenscanner und schließt hierdurch eine Sicherheitslücke besonders für unerfahrene Anwender. Erkannte der Windows Defender bisher nur Spyware, soll er nun auch herkömmlichen Schadcode wie Viren, Würmer und Trojaner finden. Microsoft hat es dabei verstanden, die bereits unter Windows 7 erfolgreich eingeführten Security Essentials vollständig in den Windows Defender zu integrieren.

Auch der unter Internet Explorer 9 eingeführte SmartScreen-Filter zum Schutz vor Bedrohungen aus dem Internet erhält eine größere Aufgabe im neuen Betriebssystem: Diente der SmartScreen-Filter im Internet Explorer bisher nur dazu, vor gefährlichen Downloads im Internet Explorer selbst zu warnen, so wird ab Windows 8 jedes aus dem Internet geladene Programm beim Start einer sorgfältigen Prüfung unterzogen. Windows SmartScreen ergänzt so bereits vorhandene Sicherheitsfeatures wie die UAC (Benutzerkontensteuerung) oder die Windows Firewall sinnvoll. Zur Überprüfung der Dateien hält Microsoft eine Datenbank bereit. Ist ein Programm in der Datenbank als potenziell unsicher eingestuft, erscheint ein Fenster mit ei-

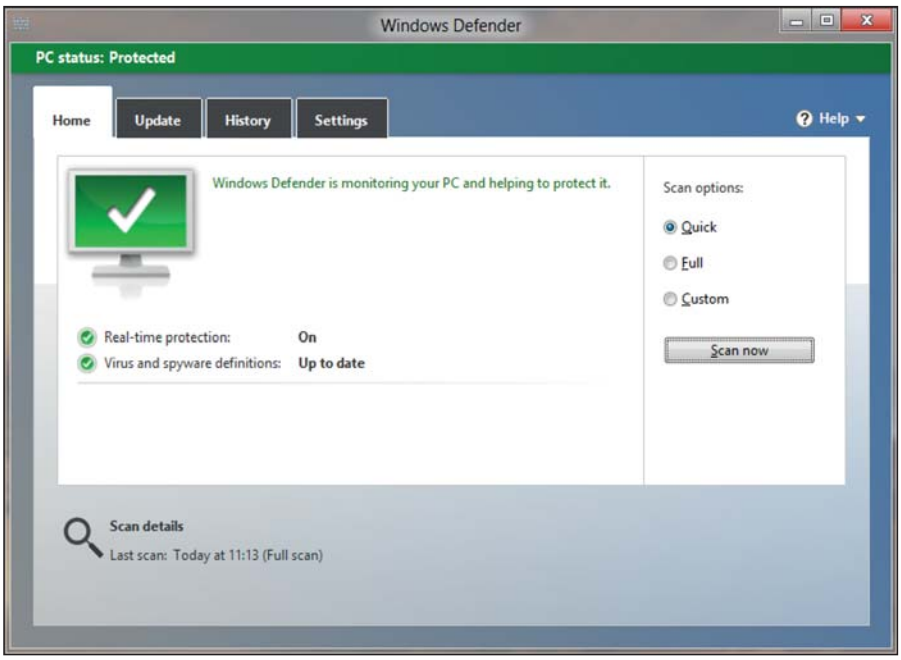


Bild 1: In Windows 8 hat Microsoft den Windows Defender zu einem vollwertigen Virenscanner ausgebaut

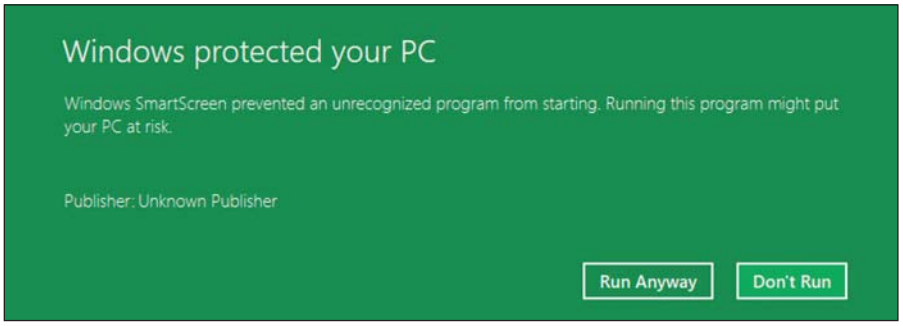


Bild 2: SmartScreen prüft Anwendungen aus dem Web vor dem Start

nem Warnhinweis. Gilt das Programm hingegen als sicher und vertrauenswürdig, so erscheint kein Warnhinweis mehr.

Zurück auf Los

Mussten Nutzer unter vielen Vorgängerversionen von Windows 8 nach einer fehlerhaften Installation, einem Treiberkonflikt oder einem Systemabsturz das Betriebssystem neu installieren, bietet Windows 8 nun zwei völlig neue und durchaus interessante Features an. So ist es dem Benutzer möglich, sein System bei einem Problem mit Hilfe des Refresh-Buttons (Auffrischen) auf den Urzustand zurückzusetzen und dabei alle Benutzerkonten und persönliche Daten beizubehalten. Lediglich durch den Benutzer installierte Applikationen, mit Ausnahme von Metro-Apps, gehen verloren. Mithilfe des Reset-Buttons (Originaleinstellung) ist es dem Benutzer gar möglich, den Computer auf einen kompletten Urzustand zurückzusetzen – so als wäre das Betriebssystem gerade erst installiert worden. Mithilfe dieser Features dürfte es zukünftig höchstwahrscheinlich nur noch eine einzige Betriebssysteminstallation im Laufe eines Windows-Rechnerlebens geben.

Einen immer wieder auftauchenden Angriffspunkt stellen PDF-Dateien dar. Bei mehr als der Hälfte aller gezielten Angriffe aus dem Internet kommen manipulierte PDF-Dateien zum Einsatz. In der Regel werden die PDF-Dokumente als E-Mailanhänge verschickt, die mehr oder weniger auf die Empfänger zugeschnitten sind. Die Infizierung erfolgt dann meist über eine JavaScript-Funktion, die innerhalb der präparierten PDF-Datei aufgerufen wird. Oft waren hierbei in der Vergangenheit Virenscanner machtlos, da sie diese Art von Angriff nicht erkannten. Der neue Windows Reader soll unter Windows 8 zumindest die Abhängigkeiten von bisheriger Drittanbieter-Software wie Adobe- oder Foxit Reader minimieren. Über integrierte Updatemechanismen verspricht Microsoft eine zeitnahe und automatische Aktualisierung der Reader-Komponenten. Die Software zeigt dabei im neuen Metro-Style PDF-Dokumente in drei möglichen Ansichten an.

Sicheres Booten

Windows 8 unterstützt künftig das Unified Extensible Firmware Interface (UEFI), den Nachfolger des PC-BIOS. In Kombination mit SecureBoot sorgt es dafür, dass nur signierte Betriebssysteme starten können, für die ein Schlüssel in der Firmware des Systems existiert. Voraussetzung hierfür ist jedoch ein kompatibles Mainboard mit UEFI und der Firmware-Version 2.3.1. Damit soll verhindert werden, dass Schadcode den Bootsektor eines Systems infiziert oder ein System mit einer Live-CD gestartet wird, um etwa den Passwortschutz oder eine Verschlüsselung auf dem eigentlich installierten Betriebssystem auszuhebeln.

Die integrierte Verschlüsselungslösung erhält auch unter Windows 8 einige neue und interessante Verbesserungen. So wird es unter Windows 8 nun auch erlaubt sein, BitLocker vor der eigentlichen Betriebssysteminstallation mit dem Windows Pre-Installation Environment (WinPE) zu konfigurieren. Darüber hinaus soll es möglich sein, neben der gesamten Festplatte nun auch den lediglich belegten Festplattenspeicher zu verschlüsseln – mit dieser Funktion will Microsoft das Verschlüsseln großer Festplatten beschleunigen. In Windows 8 können Nutzer zudem ohne administrative Berechtigungen ihre BitLocker-Konfiguration – etwa das Ändern von TPM und PIN – eigenständig vornehmen.

Windows To Go

Eine absolute Neuerung unter Windows 8 stellt Windows To Go dar. Windows To Go ist quasi ein herkömmliches Windows 8 – mit dem Unterschied, dass es nicht auf einer internen Festplatte, sondern auf einem mobilen Datenträger läuft. Der Datenträger wird dabei mit einem vollständig funktionsfähigen Windows 8 konfiguriert. Vorteil: Windows To Go lässt sich auf nahezu jedem System starten. Dies soll es IT-Organisationen erleichtern, den Trend "Bring your own Device" zu unterstützen. Einziger Wermutstropfen: Windows To Go bleibt vorerst Windows 8 Enterprise-Kunden vorbehalten. Daher steht es nur Kunden mit Volumenlizenzen zur Verfügung.

Der unter Windows 7 und Server 2008 R2 eingeführte Direct Access schließlich wird zukünftig um weitere Features erweitert. Benutzer benötigen hierdurch kein dediziertes VPN mehr, um sich mit dem Firmennetz zu verbinden. Neben einer besseren Anbindung an bestehende Internetdienste sollen externe Benutzer einen schnelleren und vor allem sicheren Zugriff auf das Firmennetz erhalten. Mithilfe verschiedenster Einstiegspunkte sollen Zugriffe für Benutzer vereinfacht, optimiert und abgesichert werden.

Fazit

Windows 8 setzt in Sachen Sicherheit dort an, wo Windows 7 aufgehört hat. Microsoft versteht es anscheinend, das Betriebssystem mit neuen und erweiterten Features um sinnvolle und notwendige Sicherheitsmechanismen zu ergänzen. Neben der unter Windows 7 eingeführten UAC wird zukünftig auch der Windows SmartScreen dazu beitragen, dass unerwünschte und nicht vertrauenswürdige Applikationen nicht ausgeführt werden können. In puncto Sicherheit dürfte Windows 8 damit die Messlatte wieder ein Stück nach oben legen. Bewähren kann sich die Sicherheitsarchitektur jedoch nur in der Praxis. *(dr)*

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

Kurz nach der Veröffentlichung des **System Center 2012 Virtual Machine Manager** hat Microsoft ja bereits mit **Update Rollup 1** die ersten **Hotfixes** bereitgestellt. Wie schätzen Sie die Lage ein, ist es ratsam, die Aktualisierung gleich vorzunehmen und wenn ja, was sollten wir dabei beachten?

Es ist auf jeden Fall empfehlenswert, die Hotfixes zum SCVMM so schnell wie möglich einzuspielen. Eine detaillierte Beschreibung der Korrekturen gibt es übrigens in der Microsoft Knowledge Base [Link-Code C7PE4]. Die Webseite listet zudem alle behobenen Fehler auf. Beachten Sie, dass im Update Rollup drei Hotfixes enthalten sind, eines für den SCVMM Management Server, eines für die Admin Console und eines für das optionale Self-Service Portal. Sollte also zum Beispiel die Admin Console auf weiteren Systemen installiert sein, müssen Sie das Update dort ebenfalls ausrollen. Im Rahmen des Update Rollup 1 haben die Entwickler aus Redmond auch eine aktualisierte Version des System Center Operations Manager (SCOM) Management Packs veröffentlicht. Besteht in Ihrem Unternehmen noch keine SCOM-Integration, können Sie das Management Pack vorab aktualisieren. Dazu müssen Sie die Dateien im Verzeichnis "C: \ Program Files \ Microsoft System Center 2012 \ Virtual Machine Manager \ ManagementPacks" ersetzen. Zusätzlich sollten Sie nach dem Management Pack-Update auf dem SCVMM Management Server noch die Registry mit der aktuellen Versionsnummer anpassen:

```
Key: HKLM \ SOFTWARE \ Microsoft \
  Microsoft System Center Virtual
  Machine Manager Server \ Setup
Entry: CompatibleMPVersion
Type: REG_SZ
Value: 3.0.6019.0
```

Zusätzliche Hinweise zur Operations Manager-Integration finden Sie unter [Link-Code C7PE5]. *(Michel Lüscher/ln)*

SERVER TALK

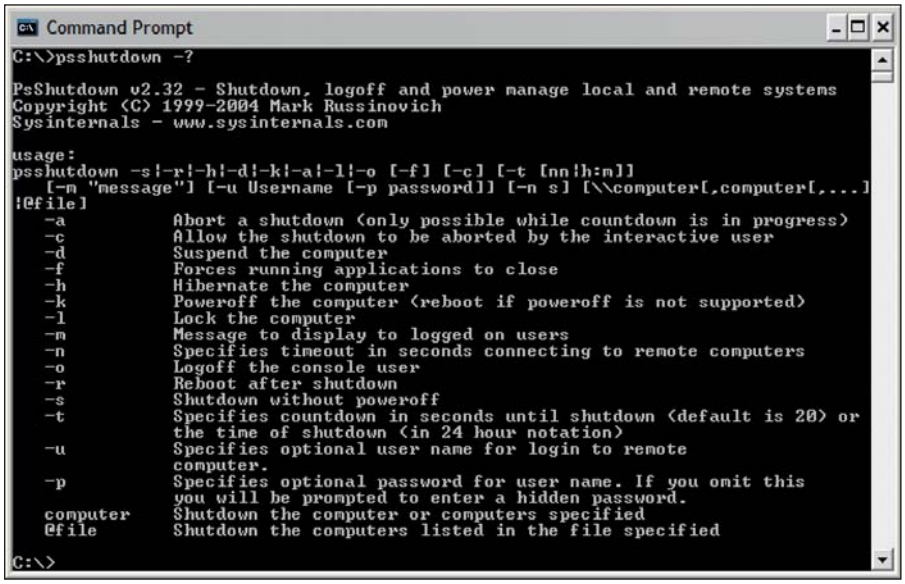
Weitere Informationen zu Server 2008 R2 und Hyper-V finden Sie auf www.server-talk.eu

Unter **Windows 7** bietet das Kontextmenü beim Auswählen einer Datei mit der rechten Maustaste ja unter anderem die Option **Senden an**. Leider lässt sich über diesen Punkt aber nicht direkt ein **Verzeichnis auswählen**, in das die ausgewählt Datei verschoben oder kopiert wird. Nun habe ich bei einem Kollegen gesehen, dass genau diese beiden Funktionen unter den Namen **In Ordner kopieren** beziehungsweise **In Ordner verschieben** in seinem Kontextmenü vorhanden sind. Wie hat er das hinbekommen?

Diese Einträge fügen Sie ein, indem Sie zunächst über *regedit* im Feld "Ausführen" in die Registry wechseln. Im Registrierungseditor navigieren Sie dann zum Schlüssel "HKEY_CLASSES_ROOT \ AllFilesystemObjects \ Shellex \ ContextMenuHandlers". Hier definieren Sie zwei neue Unterschlüssel. Dazu klicken Sie mit der rechten Maustaste auf "ContextMenuHandlers", wählen im Kontextmenü "Neu / Schlüssel" und geben dem ersten Schlüssel die Bezeichnung "{C2FBB630-2971-11D1-A18C-00C04FD75D13}". Legen Sie einen zweiten Schlüssel an, den Sie mit "{C2FBB631-2971-11D1-A18C-00C04FD75D13}" benennen. Nach dieser Registry-Ergänzung erscheinen im Kontextmenü aller Verzeichnisse und Dateien die Optionen "In Ordner kopieren" und "In Ordner verschieben". *(ln)*

Die **Vorschau von Windows 7** auf **geöffnete Fenster,** wenn der Nutzer die Maus in der Taskleiste auf das Symbol eines aktiven Programms bewegt, ist ja recht praktisch. Die Preview ist in den Standardeinstellungen aber recht winzig, so dass ich etwa bei **mehreren geöffneten Fenstern** eines Textverarbeitungsprogramms kaum erkennen kann, welches Dokument nun in welchem Fenster zu finden ist. Lässt sich die Größe der Vorschaufenster irgendwie verändern?

Um die Größe der Vorschaufenster individuell anzupassen, öffnen Sie mit *regedit* die Registry und navigieren zum Schlüssel "HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Explorer \ Taskband". Klicken Sie mit der rechten Maustaste auf eine freie Stelle des Fensters rechts. Im Kontextmenü wählen Sie nun "Neu / DWORD-Wert (32 Bit)" und benennen den Eintrag mit "MinThumbSizePx". Klicken Sie anschließend doppelt darauf, aktivieren Sie "Dezimal" und setzen Sie als Wert "500". Bestätigen Sie mit "OK" und melden sich neu an. Die Größe des Preview-Fensters sollte nun den neuen Wert besitzen. *(ln)*



Das Kommandozeilen-Tool "psShutdown" stellt eine Vielzahl von Schaltern bereit, mit denen sich Rechner auch remote gezielt herunterfahren lassen können

Wir nutzen im Unternehmen das Kommandozeilen-Tool **psShutdown**, um Server und Clients **herunterzufahren** beziehungsweise neu zu **booten**. Ich bin mit der **Syntax** des Programms noch nicht so vertraut, könnten Sie vielleicht einige Beispiele zu seiner Verwendung auflisten?

Zunächst einmal sollten Sie beachten, dass "psShutdown" ein sehr mächtiges Werkzeug ist und dass Sie über den Einsatz von Wildcards etwa mit dem Befehl

```
psshutdown \\* -s -t 30
```

nach einem Countdown von 30 Sekunden alle Rechner einer Domäne herunterfahren können. Damit Ihnen das zumindest nicht ganz aus Versehen passiert, besteht das Werkzeug stets auf die Eingabe des Schalters, auf welche Weise der Shutdown (Neustart, Ausschalten, Energiesparmodus et cetera) erfolgen soll. Eine genaue Erklärung sämtlicher Schalter erhalten Sie auf der Download-Seite [Link-Code C7PE6] des Tools. Mit dem Kommando

```
psshutdown.exe \\Name des Rechners
  -s -f -c -t 20:15 -m "Achtung, um
  20:15h fährt dieser Rechner
  herunter"
```

etwa veranlassen Sie, dass der betreffende PC um 20:15 Uhr (-t) mit einer vorherigen Warnmeldung (-m) herunterfährt (-s) und dabei sämtliche laufenden Programme ohne Sicherungsmöglichkeit beendet (-f). Der Schalter "-c" erlaubt es dem Nutzer allerdings, den Shutdown über ein Cancel-Feld abzubrechen. *(ln)*

Microsoft Exchange

Wir nutzen **Exchange Server 2010** in unserem Netzwerk. Die meisten Clients haben wir bereits auf **Outlook 2010** aktualisiert. Doch bei einigen ist dies nicht der Fall beziehungsweise nicht so schnell möglich; auf diesen nutzen wir noch die **Version 2003**. Obwohl wir die Verschlüsselung aktiviert haben, kommt es immer wieder zu **Problemen mit dem E-Mailabruf**. Woran könnte der Fehler noch liegen?

Exchange Server 2010 nutzt zur Kommunikation mit den MAPI-Clients eine verschlüsselte Verbindung. Outlook 2003 jedoch verwendet in den Standardeinstellungen keine Verschlüsselung, weshalb der Kontakt zum Server üblicherweise scheitert. Stellen Sie zunächst sicher, dass Sie wirklich die Verschlüsselung aktiviert haben. Dies lässt sich auf zwei Wegen durchführen: Setzen Sie noch eine größere Anzahl an Outlook 2003-Clients ein, können Sie einen Registry-Schlüssel per Gruppenrichtlinien verteilen. Hierbei müssen Sie den Key "EnableRPCEncryption" vom Typ REG_DWORD auf "1" setzen. Sie finden den Wert unter "HKEY CURRENT USER / Software / Policies / Microsoft / Office / 11.0 / Outlook / RPC". Handelt es sich dagegen nur um einen oder wenige Clients, prüfen Sie die Verschlüsselung einfach per Menü nach. Sie finden die Einstellung unter "Extras / E-Mailkonten / Exchange Server / Weitere Einstellungen / Sicherheit". Sollte dies keinen Erfolg bringen, schalten Sie testweise die Verschlüsselung auf Ihrem Exchange Server ab, indem Sie den Befehl

```
Set-RpcClientAccess -Server Name des
  Client Access Servers  -Encryp-
  tionRequired $false
```

eingeben. Sollte der Zugriff dann immer noch haken, könnte es an den RPC-Zugriffen liegen. Die Client Access Server (CAS) beschränken die Anzahl an gleichzeitigen Verbindungen je Client nämlich auf 20. Greifen die User mit ihrem Mailclient jedoch gleichzeitig auf mehrere Postfächer oder ihre Kalender zu, kann die Anzahl an Connections diesen Wert übersteigen. Mit dem Befehl

```
Get-LogonStatistics -Server Server-
  FQDN -Identity Alias oder SMTP-
  Adresse | fl applicationid
```

fragen Sie die entsprechenden Statistiken für die einzelnen User ab. Den Wert, nachdem Sie Ausschau halten müssen, finden Sie unter der Bezeichnung "MSExchangeRPC". Reicht die Anzahl an Connections nicht aus, erhöhen Sie den Wert einfach mit dem Befehl

```
Set-Throttlingpolicy -RCAMaxConcur-
  rency Anzahl an Connections
```

und überprüfen Sie, ob die Verbindung nun klappt. Der Maximalwert liegt bei zwei Millionen und sollte damit genügend Luft nach oben bieten. Um die Änderungen wirksam werden zu lassen, müssen Sie abschließend noch den Dienst "MSExchangeRPCClientAccess" auf Ihren CAS-Servern neu starten. Hilfreiche Fehlermeldungen finden Sie natürlich stets in den Logdaten des Exchange Servers. Wie Sie diese optimal auswerten, können Sie in IT-Administrator Ausgabe 02/2012 nachlesen. *(dr)*

Google Chrome

Oft ist es ja der Browser mit einem Dutzend geöffneter Tabs, der ein System ordentlich in die Knie zwingen kann. Über den **Task-Manager** von Windows lässt sich dann zwar erkennen, dass der Browser alles zum Stocken bringt – **welcher Tab** beziehungsweise **welche Webseite** aber hauptsächlich dafür verantwortlich ist, lässt sich hierüber nicht erkennen. Gibt es irgendeine Möglichkeit herauszubekommen, welche Tabs das System in welchem Maße beeinflussen?

Zumindest bei Googles Browser Chrome existiert eine einfache Möglichkeit, um sich über das Innenleben des Browsers zu informieren. Drücken Sie hierzu einfach "SHIFT + ESC" und der Chrome-eigene Task-Manager erscheint auf dem Bildschirm, der Sie detailliert über den CPU- und Speicher-Hunger einzelner Tabs, aber auch von Browser-Add-Ons informiert. Ein Rechtsklick in die Tabelle bringt zudem weitere Anzeigeoptionen wie etwa den Skript-Cache oder die Vorgangs-ID zu Tage. Der im Fenster angezeigte Link "Statistiken für Nerds" öffnet einen eigenen Tab mit einer Übersicht über den verbrauchten Speicher. Diese Anzeige können Sie auch direkt über die Navigationsleiste mit *chrome://memory* aufrufen. *(ln)*

Linux

Ich möchte mein unter **Linux erzeugtes X.509 Benutzer-Zertifikat** auf einem **Webbrowser unter Windows** importieren. Laut Beschreibung soll dies über eine **PKCS#12-Datei** stattfinden. Wie kann ich diese aus meinen beiden Zertifikatsdateien unter Linux erzeugen?

Wie so oft hilft auch hier das Schweizer Taschenmesser im Krypto-Bereich weiter: OpenSSL. Mit dem folgenden Befehl erstellen Sie aus dem Zertifikat und dem dazugehörigen privaten Schlüssel eine entsprechende PKCS#12-Datei. Der OpenSSL-Aufruf sieht wie folgt aus:

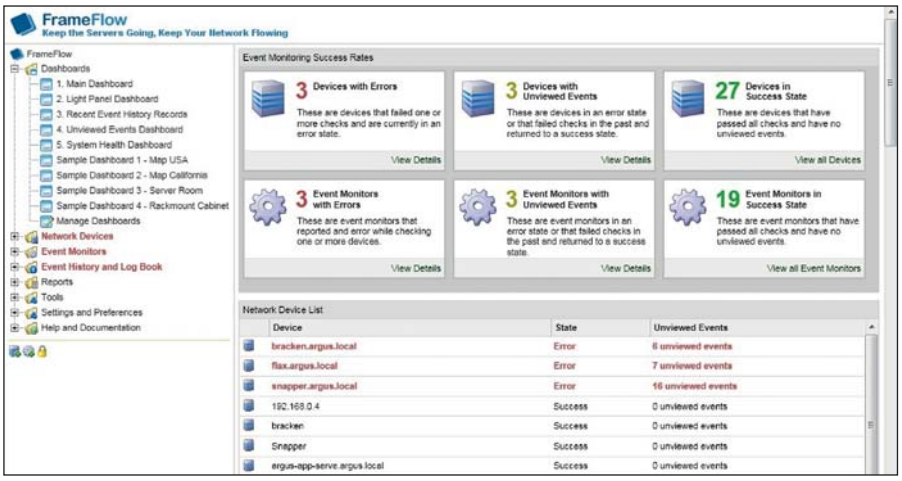
```
# openssl pkcs12 -in user.crt -inkey
  user_key.pem -export -out user.p12
```

Die so erstellte PKCS#12-Datei können Sie dann wie gefordert in Ihrem Webbrowser importieren. *(Thorsten Scherf/ln)*

Tools

Der Weg zum dauerhaften **Monitoring der IT-Infrastruktur** zur Sicherstellung der geplanten Performance und Verfügbarkeit ist mit zahlreichen Herausforderungen für den Admin gepflastert. Ohne ein speziell für diese Aufgabe zugeschnittenes Werkzeug muss sich der IT-Verantwortliche händisch durch zahllose Log-Files kämpfen. Nutzt er hingegen ein Monitoring-Tool, muss er sich unter Umständen mit einer übermäßig komplexen Konfiguration oder der Verteilung von Agenten auf die Zielsysteme auseinandersetzen. Und hat er seine Überwachungsinfrastruktur dann zum Laufen gebracht, gibt es nicht wenige Tools, deren Ergebnisdarstellung kaum übersichtlicher ist als die eingangs erwähnte Suche in Log-Files.

Da ist es erfreulich, wenn mit **FrameFlow** ein Werkzeug bereitsteht, das nicht nur einfach zu bedienen ist und die Monitoring-Ergebnisse übersichtlich darstellt, sondern auch kostenlos ist. FrameFlow kommt dabei ohne Agenten aus und zeigt sich zudem in Sachen Systemanforderungen (2 GByte RAM und 5 GByte freier Plattenplatz) genügsam. Schon bei der Installation zeigt sich das Web-basierte Werkzeug von seiner besten Seite und sieht dank HTML5 ganz und gar nicht wie eine typische Browser-Anwendung aus. Doch auch die Funktionalität steht dem in nichts nach und schon bei der Ersteinrichtung hilft die Anwendung dem Administrator, indem sie beispielsweise ermöglicht, alle **Subnetze nach verfügbaren und zu überwachenden Host-Rechnern zu durchforsten**. Darüber hinaus lassen sich Websites oder SQL Server-Instanzen per SNMP in die Überwachung einbinden. Hier ist die freie Version aber in bestimmten Gebieten limitiert und es werden kostenpflichtige Add-Ons notwendig. Dies ist das Geschäftsmodell des Anbieters, FrameFlow funktioniert jedoch auch ohne diese bepreisten Erweiterungen in den meisten Fällen tadellos. Nach dem Setup präsentiert sich dem Nutzer die aufgeräumte GUI, die sich aus einem Navigations- und einem Ergebnisbereich zusammensetzt. Über die Navigation lassen sich die typischen **Monitoring-Werkzeuge wie Dashboards, Reports oder Events** erreichen. Dabei lässt sich jeder Navigationspunkt per Rechtsklick schnell ansteuern, um beispielsweise einen neuen Report zu erstellen. Administratoren mit informationssüchtigen Vorgesetzten werden sich dabei sicher über die einfache Möglichkeit freuen, ein Management-Summary zu erstellen. Auch lassen sich die **Dashboards weitgehend individualisieren**, so dass es etwa möglich ist, sich eine Anzeige zu gestalten, deren Aussagen sich auf die Verfügbarkeit der Systeme fokussiert. Selbstverständlich erhält der Admin dabei alle gewohnten Status-Meldungen zu den Geräten im Netzwerk. Und auch die Konfiguration der Überwachung eines neuen Geräts ist mit wenigen Klicks ebenso erledigt wie die gezielte Filterung der Ergebnisse. FrameFlow ist lauffähig unter Windows Server 2003 und 2008 / 2008 R2 oder Windows XP, Vista und 7. Überwachen lassen sich Windows-, Linux- und BSD-Betriebssysteme sowie Webserver und Netzwerkkomponenten. Der Download ist kostenlos und ohne Registrierung möglich, lediglich die

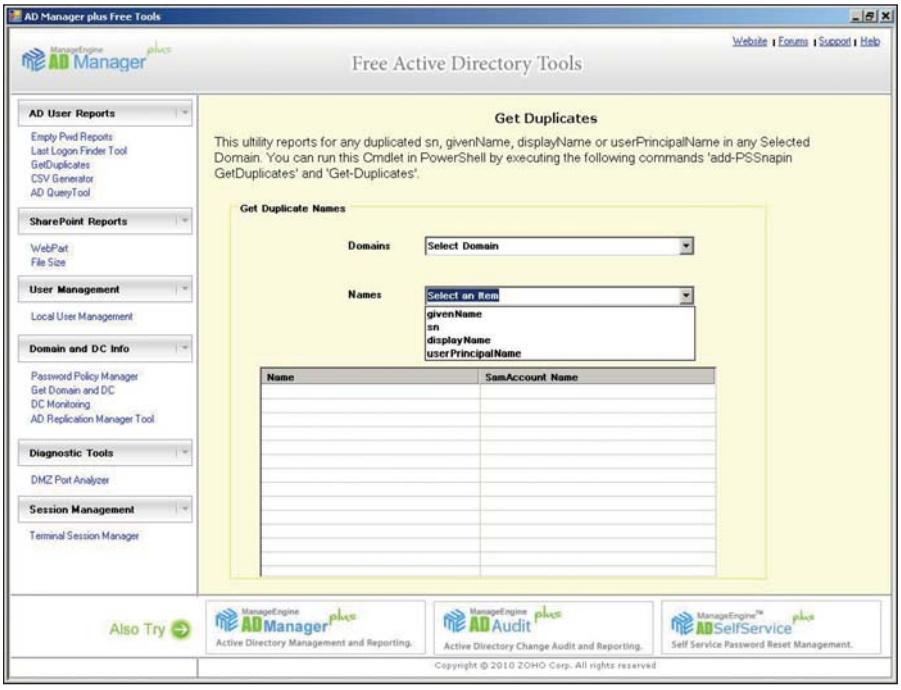


FrameFlow besticht als kostenloses Tool mit einer professionellen Oberfläche und ebensolchen Monitoring-Fähigkeiten

erwähnten Add-Ons müssen bei Bedarf kostenpflichtig erworben werden. *(jp)*
Link-Code: C7PE1

Obwohl Microsofts **Active Directory** mittlerweile das Teenager-Alter erreicht hat, plagen sich Administratoren noch immer mit der **manuellen Erledigung von Routineaufgaben** herum. Oder der Zugriff auf wichtige Informationen ist mit Bordmitteln nicht oder nur eingeschränkt möglich. Dazu zählt beispielsweise die Suche nach leeren Passwörtern oder die Information, wann sich ein bestimmter Anwender zum letzten Mal angemeldet hat. Sind solche Daten aus dem Active Directory zu generieren, muss der Administrator neben seinem Know-how auch unverhältnismäßig viel Zeit aufbringen.
Mit weitaus weniger Zeiteinsatz erledigen Admins derartige Aufgaben unter Zuhilfenahme der freien **Active Directory Tools** von ManageEngine. Dieser Werkzeugkoffer umfasst insgesamt 13 Tools, die dem IT-Verantwortlichen bei speziellen Verwaltungsaufgaben im Active Directory helfen. Der **Local User Manager** erlaubt es, User hinzuzufügen und zu entfernen, zu betrachten und zu (ent-)sperren sowie Passwörter zurückzusetzen. Parallel findet der **Empty Password Reporter** leere Passwörter und hilft so, die Sicherheit zu erhöhen. Ergänzend dazu setzt der **Password Policy Manager** Richtlinien bei der Erstellung von Passwörtern durch. Der **Last Logon Reporter** ermittelt, wann sich ein Anwender zum letzten Mal im Netz befand. Nützlich ist sicher auch der **AD Replication Manager**, der es erlaubt, manuell die Replikation bestimmter Daten zwischen den Domaincontrollern zu erzwingen. Und zur Überwachung der Domaincontroller stehen zwei Werkzeuge bereit: **DC Monitor** und **Domain und DC Roles Reporter**, die das Monitoring der Active Directory-Infrastruktur erleichtern. Weitere Werkzeuge erzeugen spezielle Reports, helfen bei der SharePoint-Integration oder der Terminalserver-Verwaltung. Die Version 4.4 der AD-Tools ist nach einer kurzen Registrierung kostenlos verfügbar. *(jp)*
Link-Code: C7PE2

Unternehmen, die ihre IT auf Basis von **VMware oder Hyper-V virtualisieren,** haben bis zum Projektende gewiss eine nicht



Die wilde 13: ManageEngines Set von Active Directory-Tools hilft bei wichtigen Verwaltungsaufgaben im Verzeichnisdienst

unerhebliche Summe Geld in die Hand genommen und somit sollte das Budget eigentlich auch noch für eine begleitende **Monitoring- und Management-Lösung** ausreichen. Ist die Installation jedoch eher klein oder dient nur zu Testzwecken, macht der Einkauf eines solchen Produkts in der Regel wenig Sinn.
Hier hilft dem IT-Verantwortlichen das kostenlose Tool **Veeam ONE Free Edition**. Die Software bietet dabei alle Kernfunktionen der lizenzpflichtigen Variante für eine unbegrenzte Anzahl an Hosts und vCenter-Servern: **Monitoring, Dokumentation und Reporting**. Für das Monitoring bietet das Tool **125 vordefinierte Alarmmeldungen**, die alle mit einer ausführlichen Wissensdatenbank verknüpft sind und so das Troubleshooting merklich erleichtern. Insbesondere die Warnmeldungen aus dem Bereich "Storage" sind hilfreich, wenn virtuelle Maschinen die Limits ihrer virtuellen Disks sprengen. Verteilt werden solche Meldungen von Veeam One per SNMP oder E-Mail. Nützlich ist auch die **umfassende Dokumentation** der virtuellen Infrastruktur, die die Software direkt nach der Erstinstallation anlegt. So erhält der Administrator einen guten Überblick seiner Topologie und kann diese beispielsweise mit Performance-Daten verknüpfen. Und auch Veeam One trägt dem Informationshunger der Management-Ebene Rechnung und erlaubt die einfache Erstellung von Management-Übersichten als Teil der Reporting-Funktionen der Software. Wer einen besonders neugierigen Chef hat, kann ihm (oder ihr) sogar den Zugriff auf einzelne Dashboards einrichten. Der Admin selbst kann sich mit den vollständig anpassbaren Berichten genau die Ansichten bauen, die er für die optimale Verwaltung der Infrastruktur benötigt. Darüber hinaus bietet Veeam ONE Free Edition auch die Möglichkeit, Hosts und virtuelle Maschinen anhand der Nutzung durch die jeweiligen Fachabteilungen zu sortieren und so beispielsweise nutzungsbezogene Abrechnungsmodelle einzurichten. *(jp)*
Link-Code: C7PE3

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

Juristischer Rahmen zur IT-Sicherheit

Nicht alles kann, aber vieles muss

von Michael Bock

Häufig ist der Geschäftsführung oder den für IT-Sicherheit Verantwortlichen nicht bewusst, dass und – wenn ja unter welchen rechtlichen Gesichtspunkten – sie gesetzlich dazu verpflichtet sind, bestimmte technische und organisatorische Maßnahmen zur Gewährleistung eines sicheren Betriebs der unternehmensinternen IT-Infrastruktur zu treffen. Unternehmen verstehen heute IT-Sicherheit immer noch weitgehend als Thema der Bereiche Technik und Organisation. Nur wenige Experten unter den IT-Verantwortlichen haben erkannt, dass das Spielfeld der IT-Sicherheit neben dem Bereich Technik und Organisation auch aus dem Bereich Recht besteht. Dieser Beitrag zeigt die rechtlichen Anforderungen in Fragen der IT-Sicherheit auf.

Rechtliche Anforderungen zur IT-Sicherheit können sich aus dem Wirtschaftsverwaltungsrecht, dem Datenschutzrecht oder aus dem Europäischen Recht ergeben. Konkret können beispielsweise folgende Vorschriften relevant sein: § 109 TKG, § 9 BDSG, Anlage zu § 9 BDSG, § 91 Abs.2 AktG, § 25a Abs. 1 Nr. 3 KWG, § 33 WpHG. Manche Vorschriften sind nur anwendbar, wenn das Unternehmen in bestimmten Bereichen tätig ist oder bestimmte Dienstleistungen anbietet wie Telekommunikationsdienste oder Finanzdienstleister. Andere hingegen gelten für alle Unternehmen (etwa § 9 BDSG) und für Behörden finden sich vergleichbare (oder zusätzliche) Vorschriften im Landesrecht.

Gemäß § 9 BDSG sind öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, dazu verpflichtet, die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um die Einhaltung der Regelungen des BDSG zu gewährleisten. Die Datensicherheitsanforderungen des BDSG sind in der Anlage zu § 9 Satz 1 BDSG weiter ausgestaltet. Als verschiedene Aspekte der Datensicherheit sind dort eine den Umständen nach geeignete Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle und Verfügbarkeitskontrolle sowie die getrennte Verarbeitung personenbezogener Daten mit unterschiedlicher Zweckbestimmung (sog. Trennungsgebot) genannt. Gemäß § 9 Satz 2 BDSG sind Maßnahmen nur dann erforderlich, wenn der mit ihnen verbundene Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Dabei ist davon auszugehen, dass der einem Unternehmen zumutbare Aufwand proportional zur Sensibilität der zu sichernden personenbezogenen Daten steigt. Dies gilt insbesondere hinsichtlich der Sicherung personenbezogener Daten vor einer Einsichtnahme durch Dritte und damit für die Aspekte der Zutritts-, Zugangs-, Zugriffs- und Weitergabekontrolle.

Unternehmen werden es im Übrigen auch vermeiden wollen, in die Situation zu kommen, einen etwaigen Datenverlust im Sinne von § 42 a BDSG der Aufsichtsbehörde, den Betroffenen oder ihren Kunden melden zu müssen. Eine Sicherheitslücke in einem in Deutschland befindlichen IT-System löst unter Umständen zusätzliche Benachrichtigungspflichten nach US-amerikanischem Recht aus. Die Notwendigkeit, IT-Sicherheitsmaßnahmen zu treffen, kann sich zusätzlich aus vertraglichen Regelungen ergeben. Verarbeitet ein Unternehmen personenbezogene Daten im Auftrag, so hat der Dienstleister für eine ordnungsgemäße und sichere Datenverarbeitung einzustehen. Verschlüsselungen und andere Sicherheitsmaßnahmen bei der elektronischen Übertragung müssen immer dem Stand der Technik entsprechen (vergleiche Anlage zu § 9 BDSG). Werden Vertraulichkeitsvereinbarungen (NDA) geschlossen und kommen diese Informationen einer Partei aufgrund von Fahrlässigkeit (§ 276 BGB) abhanden, haftet das Unternehmen möglicherweise zusätzlich mit einer Vertragsstrafe.

Datenschutz vs. Datensicherheit

Datenschutz ist alles, was an rechtlichen Vorgaben (insbesondere aus den Datenschutzgesetzen, aber auch aus dem Strafgesetz) von den Unternehmen oder Behörden zu beachten beziehungsweise einzuhalten ist. Die Umsetzung des Datenschutzes erfordert technische, rechtliche oder organisatorische Maßnahmen. Da-

tensicherheit bezeichnet die technisch-organisatorische Umsetzung der rechtlichen Vorgaben und deren Implementierung in das operative Tagesgeschäft. Der Datenschutz ist dabei in verschiedenen Gesetzen kodifiziert. Diese Gesetze enthalten Verhaltenspflichten. Bei Verstößen gegen manche dieser Verpflichtungen sehen die Gesetze die Möglichkeit der Beanstandung durch die Aufsichtsbehörde oder den Erlass von Bußgeldern vor und sie können teilweise auch strafrechtlich verfolgt werden. Darüber hinaus sollten Unternehmen Datenschutzgesetze auch beachten, um sich nicht, wie bereits genannt, Schadensersatz- und Haftungsansprüchen auszusetzen. Auch kann das öffentliche Ansehen eines Unternehmens durch Datenschutzpannen Schaden nehmen. Mittlerweile gibt es Internetseiten, die solche Pannen systematisch erfassen und offenlegen.

Risiken bei mangelnder IT-Sicherheit

Mit der zunehmenden Vernetzung und Komplexität von IT-Systemen steigt das Gefährdungspotential für diese Infrastruktur an. Auch wenn in der Vergangenheit spektakuläre Fälle an die Öffentlichkeit gelangt sind, so ist die Umsetzung von vollständiger IT-Sicherheitspolitik heute noch nicht Realität. Eine Gefahr für das Unternehmen kann sich aus ganz unterschiedlichen Richtungen ergeben. Wer seinen Mitarbeitern beispielsweise den Zugang zum Internet am Arbeitsplatz eröffnet, muss nicht nur mit Kostenfolgen rechnen, wenn Arbeitszeit privat zum Surfen genutzt und die Internet-Verbindung belastet wird. Mit dem Zugang zum Internet erhalten umgekehrt auch Viren, Würmer, Trojaner und sonstige schädliche Inhalte Zugang zur IT-Infrastruktur des Unternehmens, sodass diese erheblich beeinträchtigt werden kann. Mitarbeiter können durch das Herunterladen und das Installieren nicht lizenzierter Software Urheberrechtsverletzungen begehen. Durch das Herunterladen oder das Versenden von Dateien mit extremistischen, sexistischen oder sogar pornographischen Inhalten können der Betriebsfrieden und das Ansehen in der Öffentlichkeit erheblich gestört werden. Schließlich besteht sogar die Gefahr, dass über E-Mail unkontrolliert Betriebs- oder Geschäftsgeheimnisse offenbart oder durch Mitarbeiter unkontrolliert "abgegriffen" werden können.

Die Verantwortlichkeiten innerhalb der Unternehmen sind bezüglich dieser Risiken häufig unzureichend geregelt. Bedenklich ist die nachlässige Einstellung beim Thema Corporate Compliance zum einen, weil die hohen Strafen gerade für kleinere Unternehmen schnell existenzbedrohende Ausmaße annehmen können. Es kommen neben den Bußgeldern auch Schadensersatzzahlungen, gegebenenfalls Gewinnabschöpfung sowie Honorare für Rechtsanwälte und sonstige Berater in Betracht. Zum anderen sind die Imageschäden häufig kaum zu beziffern und können nach einem einmal eingetretenen Reputationsverlust auch nur unzureichend wieder kompensiert werden.

Grenzen der Viren- und Spam-Bekämpfung

Bei der Viren- und Spam-Bekämpfung sind Persönlichkeits- und Datenschutz-

rechte zu beachten. Je nach unternehmensinterner Regelung kann sogar das Fernmeldegeheimnis nach § 88 TKG betroffen sein, welches durch § 206 StGB besonderen strafrechtlichen Schutz genießt. Datenschutzverstöße unterhalb des Fernmeldegeheimnisses können nach den §§ 43, 44 BDSG geahndet werden. Kein Arbeitgeber oder Vorgesetzter möchte sicherlich das Risiko eingehen, sich einem Strafverfahren auszusetzen. Insofern ist auf eine genaue rechtliche Absicherung der getroffenen Regelung zu achten. Welche einzelnen Rechtsgrundlagen betroffen sind, ist danach zu unterscheiden, ob die private Nutzung von E-Mails für Arbeitnehmer erlaubt ist oder nicht. Neben den datenschutzrechtlichen Fragstellungen können durch Viren- und Spam-Filter auch verschiedene Strafvorschriften verletzt werden.

Generell dürfen aus Gründen der Datensicherheit (geschäftliche) E-Mails oder ihre Anlagen gelöscht oder unterdrückt (geblockt) werden, die gefährlichen oder verdächtigen ausführbaren Code enthalten (Dateien mit bestimmten Endungen oder verschlüsselte Dateien, die nicht geprüft werden können). Wird die Löschung (Blockung) nicht selbst durchgeführt, kann dies problematisch sein, sofern dem Provider nicht explizit ein unberechtigtes Öffnen der geblockten E-Mails vertraglich verboten wurde sowie eine unverzügliche Löschung dieser Daten durch den Provider vorgesehen ist.

Nach heute wohl überwiegender Meinung ist der Mail-Provider sogar verpflichtet, eingehende Nachrichten seiner Kunden vor Virenbefall zu schützen. Er kann dies allerdings nur dann tun, wenn er in den AGB mit seinen Kunden die Berechtigung zur Prüfung der eingehenden E-Mail auf Virenbefall auch vereinbart hat, da er sonst gegen die §§ 88 TKG, 206 StGB verstoßen würde. Vereinbart werden muss auch, wie reagiert wird – also ob virenbefallene E-Mails gelöscht oder nur in Quarantäne genommen werden. Die Löschung ohne Einwilligung kann als Nachrichtenunterdrückung strafbar sein (§ 206 Abs. 2 Nr. 2 StGB). Umstritten ist, welche Vereinbarungen in Bezug auf Spam in AGB getroffenen werden können. Unzulässig ist es wohl, in AGB vorzusehen, dass Spam-E-Mails einfach nicht zugestellt werden. Das In-Quarantäne-Stellen von E-Mails dürfte hingegen zulässig vereinbart werden können. Auch bei der Gestattung privater E-Mails in Betrieben dürfen aus Gründen der Datensicherheit E-Mails oder ihre Anhänge, die ausführbare Codes enthalten, unterdrückt werden (Alternativ können auch nur die Anhänge entfernt werden).

Spam-Filter können ebenfalls das Fernmeldegeheimnis berühren. Setzen die Maßnahmen zur Spam-Erkennung und anschließenden Spam-Behandlung dagegen erst auf dem Mailclient des Mitarbeiters ein, dann kann dieser selbst über deren Ausprägung und Anwendung entscheiden. Damit ist das Fernmeldegeheimnis nicht berührt. Diese Vorgehensweise ist bei einer gestatteten Privatnutzung grundsätzlich zu wählen. Andere Verfahren sollten genauestens betrieblich geregelt werden und dem Mitarbeiter zur Kenntnis gebracht werden, eventuell ist vorher seine Einwilligung einzuholen.

Im Falle des Verbots einer privaten Nutzung von E-Mail kann die zentrale Erkennung, Blockierung und Markierung oder Löschung offensichtlicher Spam-E-Mails aus datenschutzrechtlicher Sicht zur Gewährleistung der Aufrechterhaltung des Betriebs akzeptiert werden. Sofern die Spam-Erkennung allerdings erst auf dem Server des Betriebs erfolgt, also Spam-E-Mails nach Zustellung und nicht bereits während des Übermittlungsvorgangs zurückgewiesen werden, ist zu beachten, dass auch die fälschlich als Spam erkannte E-Mail rechtlich als zugegangen anzusehen sein dürfte.

Rechtliche Aspekte bei Managed Security

Wer Vorsorge trifft, kann mit der Nutzung von E-Mail-Sicherheitslösungen als Managed Service zukünftige Ausgaben verhindern oder zumindest erheblich reduzieren (Return on Security Invest). Eine vollständige IT-Sicherheitspolitik berücksichtigt immer über die technischen Lösungen hinaus die organisatorischen Maßnahmen und insbesondere die rechtlichen Aspekte im Bereich IT-Sicherheit. Managed-Security-Lösungen müssen bei ihrer Umsetzung externe und interne Anforderungen, von gesetzlichen und regulatorischen Vorgaben bis hin zu Unternehmensrichtlinien, einhalten.

Je nach Unternehmen, Branche und Art der zu verarbeitenden Daten können zu datenschutzrechtlichen oder sicherheitsbezogenen Anforderungen eine Vielzahl weiterer Anforderungen (wie Wirtschaftsprüfungs- und Buchführungsstandards) hinzutreten. Beachtet werden sollte in jedem Fall: Liegt Auftragsdatenverarbeitung im Sinne von § 11 BDSG vor?

Werden personenbezogene Daten an einen Dritten übertragen oder erhält dieser zumindest die Möglichkeit der Einsichtnahme dieser Daten und bleibt er weisungsgebunden, wird dies meistens der Fall sein. Dann sind für privatwirtschaftliche Unternehmen die Anforderungen des § 11 BDSG einzuhalten. Hiervon betroffen sind im Besonderen die nach § 11 Abs. 1 Nr. 3 BDSG festzulegenden technischen und organisatorischen Maßnahmen sowie nach § 9 BDSG und dessen Anlage diesbezügliche Kontroll- und Dokumentationspflichten. Bei einem länderübergreifenden Datenaustausch kann sich weiterer Regelungsbedarf aus den §§ 4b ff. BDSG ergeben. Gibt es in dem Unternehmen einen Betriebsrat oder eine Personalvertretung, dann sind bestehende Mitbestimmungsrechte zwingend zu beachten (vgl. für die private Wirtschaft § 87 Abs. Nr. 6 BetrVG, § 90 BetrVG). *(dr)*

Michael Bock ist als Rechtsanwalt spezialisiert auf Informations-, Wettbewerbs-, Arbeits- und Medienrecht. Seine Kanzlei (www.rabock.de) sitzt in Willich. Im Auftrag von eleven hat er einen Compliance-Leitfaden erstellt. Mehr Infos unter www.eleven.de.

Verbindliche Regeln

Eindeutige betriebliche Regelungen und IT-Richtlinien genießen eine große Bedeutung. Insbesondere sollten diese Regelungen zum richtigen Umgang mit und zur Privatnutzung von E-Mail und Internet, zur richtigen Handhabung von Passwörtern und der IT-Infrastruktur im Allgemeinen enthalten. Arbeitsrechtliche Sanktionen sind im Verletzungsfalle durchaus möglich, wobei dem Arbeitgeber zu raten ist, durch kontinuierliche Kontrolle und Sanktionen deren Umsetzung sicherzustellen, da andernfalls eine betriebliche Übung entstehen könnte, die die vom Arbeitgeber aufgestellten Pflichten wie das Verbot der Privatnutzung von Internet und E-Mail möglicherweise entfallen lässt.

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

Aktuelle Trends und Entwicklungen bei Public Key-Infrastrukturen

Trau, schau, wem!

von Dr. Ralf Stodt

Quelle: Purwa – 123RF

PKI gibt sein Comeback im großen Stil: Da immer mehr Web- und Cloud-Dienste ihre Authentifizierung auf Zertifikate aufbauen und Letztere insbesondere auch für mobile Geräte zunehmend an Bedeutung gewinnen, sehen sich IT-Verantwortliche mehr und mehr mit dem Bedarf einer Public Key Infrastructure konfrontiert. In diesem Beitrag beschreiben wir die Komponenten einer PKI, geben Einblicke darüber, wie sich eine PKI im Eigenbetrieb sichern lässt und zeigen anhand aktueller Anwendungsszenarien die praktische Umsetzung.

Eine Infrastruktur öffentlicher Schlüssel (Public Key Infrastructure, PKI) verwaltet Zertifikate, die als Grundlage verschiedener sicherer Kommunikationsverfahren eingesetzt werden. Die PKI bildet hierbei alle Funktionen ab, die innerhalb eines Lebenszyklus von Zertifikaten notwendig sind: Identitätsprüfung, Ausstellung, Erneuerung, Validierung und Widerruf.

Die Zertifikate selbst basieren auf Schlüsselpaaren, die aus einem öffentlichen, bekannten Schlüssel und einem privaten, geheimen Schlüssel bestehen. Ein Zertifikat ist die elektronische Repräsentation dieses öffentlichen Schlüssels zusammen mit Informationen über den Inhaber sowie andere Eigenschaften des Schlüsselmaterials, die durch eine digitale Signatur der ausstellenden Instanz bestätigt werden. Als Standard kommen dabei heute fast ausschließlich Zertifikate nach IUT-T X.509 v3 (ITU Telecommunication Standardization Sector) zum Einsatz.

Schlüssel und Algorithmen

Über das zugrunde liegende asymmetrische Verschlüsselungsverfahren und dessen Kombination mit symmetrischer Verschlüsselung oder Hash-Verfahren ergeben sich vielfältige Anwendungsfälle von der Identitätsfeststellung von Personen, Geräten oder Services bis hin zur Verschlüsselung von Daten mit einem sicheren Schlüsselaustausch. So finden sich Zertifikate wie Identifizierung und Verschlüsselung von Webservices (SSL), Signatur und Verschlüsselung von E-Mails (S/MIME), Benutzeranmeldung an Rechnersystemen und Webservices (SAP) oder digitales Rechtemanagement (DRM).

Von wesentlicher Bedeutung für die Sicherheit der eingesetzten Zertifikate sind die Algorithmen der Signatur und das eingesetzte Hash-Verfahren. Ersteres wird in der Regel fast immer mit RSA und Schlüssellängen von 1.024 oder 2.048 Bit abgebildet. Alternativen wie DSA (Digital Signature Algorithm) und Modifikationen davon unter Verwendung elliptischer Verfahren (EC-DSA, EC-KDSA) finden sich zwar schon lange in Standards wie Common PKI 2.0 oder Empfehlungen des BSI wieder, jedoch ist die Verbreitung noch recht gering.

Im Bereich der Hash-Algorithmen werden die weitläufig eingesetzten SHA1-Varianten (160 Bit) sukzessive gegen längere Hash-Werte (SHA-224, -256, -384 und -512, auch bezeichnet als SHA2-Gruppe) getauscht. Hintergrund ist ein bereits 2005 dokumentiertes erfolgreiches Angriffsverfahren gegen SHA1. Nun ist aber auch bei den neueren Gruppe-2-Hash-Algorithmen aufgrund von Schwächen in der gemeinsam genutzten Merkle-Damgard-Konstruktion theoretisch das gleiche Angriffsszenario denkbar, jedoch hat sich das IETF bislang noch auf keinen Nachfolger einigen können. Demzufolge wird die IT voraussichtlich auch in den nächsten Jahren mit SHA1 und SHA2 arbeiten.

Aufbau einer PKI

Die Hauptaufgabe einer PKI besteht in der Erzeugung der oben beschriebenen Zertifikate. Dazu verfügt sie über ein eigenes Schlüsselpaar: den geheimen privaten Schlüssel der PKI, der entsprechend sicher aufbewahrt werden muss und zur Signierung aller Anträge weiterer Teilnehmer verwendet wird. Der zweite Schlüssel ist der öffentliche Schlüssel, der zur Verifizierung der ausgestellten Zertifikate genutzt wird. Diese Kernkomponente wird als CA (Certificate Authority) bezeichnet.

Zur organisatorischen Umsetzung einer PKI gehört auch eine Registrierungsstelle (RA, Registration Authority), bei der die benötigten Zertifikate beantragt werden. Für die Einreichung eines Antrags zum Ausstellen eines Zertifikates, dem sogenannten Certificate Signing Request (CSR), gibt es verschiedene Verfahren wie Self-Enrollment (manuelle Einreichung durch den Antragssteller), Auto-Enrollment (Einreichung und Signierung ohne manuelle Interaktion) oder die Ausstellung unter Einbeziehung eines sogenannten

RA-Officers. Neben der Prüfung des CSR auf Richtigkeit der enthaltenen Angaben ist die wichtigste Funktion der RA die Identitätsfeststellung des Antragsstellers, denn diese Identität stellt der Antragssteller nach erfolgter Signatur durch die CA anderen Kommunikationsteilnehmern gegenüber dar. Er nutzt damit die Vertrauensstellung der ausstellenden PKI für seinen eigenen Identitätsnachweis.

Ausgestellte Zertifikate einer PKI sind solange gültig, wie es durch die im Zertifikat definierten Gültigkeitsdaten angegeben ist oder aber bis das Zertifikat aus einem bestimmten Grund zurückgezogen wird. Gründe für den Widerruf durch die ausstellende PKI können beispielsweise die Schlüsselkompromittierung, das Ausscheiden eines Mitarbeiters, die Deaktivierung eines Dienstes, die Verwendung neuer Zertifikate mit erweiterten Eigenschaften oder gar die Kompromittierung einer CA sein. Diese Sperrung (Revocation) wird in sogenannten Widerrufslisten (CRL, Certificate Revocation List) veröffentlicht. Teilnehmer innerhalb einer zertifikatsgestützten Kommunikation überprüfen diese Listen zusätzlich zur Validierung der Zertifikatseigenschaften. Online-Verfahren ermöglichen die Gültigkeitsprüfung in Echtzeit beispielsweise im Rahmen von OCSP (Online Certificate Status Protocol) oder SCVP (Server-Based Certificate Validation Protocol). Als letzte erforderliche Komponente der technischen Infrastruktur ist die Enrollment Entity (EE) zu nennen, die das Interface zur Annahme eines CSRs darstellt. Neben webbasierten Enrollment Entities bieten PKIs auch Schnittstellen an, bei denen über APIs oder skriptbasierend weitere Systeme wie ein Smartcard Management System (CMS) zur Ausgabe von Chipkarten an Endanwender angebunden werden können. Zusätzlich gibt es Erweiterungen um Protokolle für Netzwerkgeräte zum Erzeugen eines CSR und Übermitteln eines Zertifikates von der CA zum Gerät. Das bekannteste Protokoll hierzu ist das von Cisco entwickelte SCEP-Protokoll (Simple Certificate Enrollement Protocol). Die verschiedenen Module einer PKI können je nach Anbieter der Software und Anforderung in einfachen Single-Server Setups bis hin zu weitverteilten und instanziierten Szenarien bereitgestellt werden, bei denen spezifische Dienste beispielsweise nur in dedizierten Netzsegmenten oder definierten Administratoren zur Verfügung stehen.

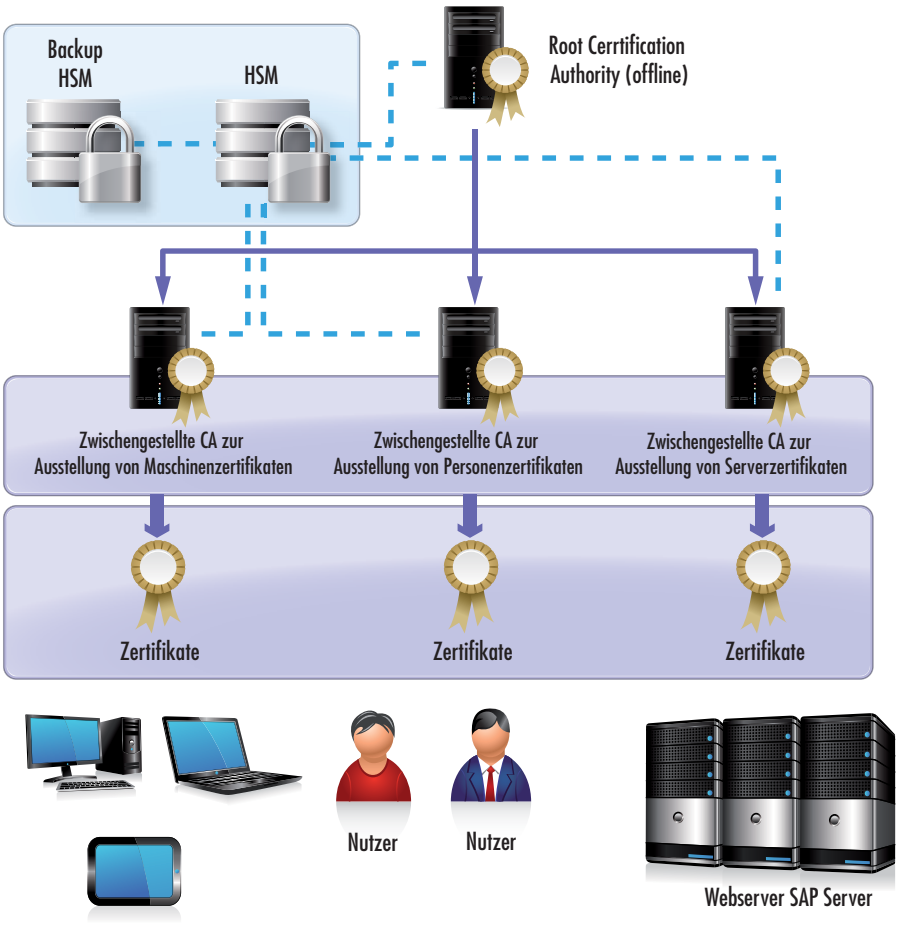


Bild 1: Schema einer zweistufigen PKI-Hierarchie mit Funktionstrennung in der Issuing-Ebene

Aus der Erfahrung heraus sollten IT-Verantwortliche beim Entwurf einer PKI jedoch darauf achten, das Setup so stringent und effizient wie möglich zu halten, da jede einzelne Komponente Einfluss auf die Sicherheit der gesamten Installation hat. Eine Beschreibung der Anforderungen an die PKI wird in Form der sogenannten Certificate Policy (CP) erstellt und durch ein Certification Practise Statement (CPS) ergänzt. Das CPS beschreibt alle technischen Komponenten sowie auch organisatorischen Prozesse innerhalb der PKI. Je komplexer eine PKI geplant wird, desto umfangreicher wird auch eine Umsetzung, die der CP entspricht.

Vertrauensbeziehungen erhöhen die Komplexität

Diese Komplexität lässt sich insbesondere durch das Vertrauensmodell zwischen verschiedenen PKI soweit steigern, dass der Betrieb einer eigenen PKI kaum noch handhabbar ist. Zu den einfacheren und am häufigsten anzutreffenden Vertrauensmodellen zählen hierarchische Strukturen, in denen die oberste Hierarchieebene durch die Root-CA dargestellt wird. Diese CA bildet innerhalb der Hierarchie den gemeinsamen Vertrauensanker zu allen unterhalb betriebenen CAs und ist somit auch durch besondere Sicherheitsmaßnahmen zu schützen.

Weiterhin ist das Modell "Web of Trust" (oder meshed PKI) zu nennen, das zum Beispiel bei OpenPGP anzutreffen ist. Des Weiteren gibt es Cross- und Bridge-Architekturen. Während bei einer Cross-PKI alle CAs untereinander vertrauen müssen, verlagert man diese Vertrauensfeststellung bei der Bridge-CA auf eine einzelne CA, die keine Zertifikate ausstellt, sondern nur als Vertrauensanker dient. In Unternehmen sind in der Regel hierarchische Strukturen anzutreffen, ein Standard-Design geht von zwei bis maximal drei Ebenen aus. Dies wird im Wesentlichen bestimmt durch die Größe des Unternehmens, unter-

schiedliche Verwaltungseinheiten oder auch regulatorische Anforderungen. Typischerweise wird sowohl innerhalb der Hierarchieebene als auch bei den ausstellenden CAs nach Verwendungszweck der Zertifikate oder anhand der Unternehmensstruktur getrennt.

Auch die PKI benötigt Schutz

Ein häufig anzutreffendes Bild ist eine bedarfsorientiert installierte PKI auf der Grundlage der Microsoft Certificate Services, die ohne Hierarchie direkt als Enterprise-PKI im Active Directory des Unternehmens dient. Oft werden solche Installationen auch in virtuellen Instanzen bereitgestellt, dadurch liegt ein hohes Missbrauchspotenzial vor. Zudem ist bei diesen Installationen auch das Rollenmodell für den Zugriff auf die PKI nur unzureichend umgesetzt, sodass die Ausstellung von Zertifikaten, Modifikation von Vorlagen oder der Zugriff auf archiviertes Schlüsselmaterial unkontrolliert erfolgen kann. Einfache Grundregeln zur sicheren Implementierung einer eigenen PKI sehen also neben dem Schutz des Schlüsselmaterials auch ein zum Unternehmen passendes Rollenkonzept zur Administration vor.

Zuerst sollte innerhalb der PKI-Hierarchie die Root-CA als Offline-System betrieben werden und das Schlüsselmaterial durch Splittung der Schlüssels in verschiedene Teile oder die Auslagerung auf dedizierte Schlüsselspeicher (HSM, Hardware Security Module) geschützt werden, Gleiches gilt natürlich auch für die privaten Schlüssel der untergeordneten CAs. Für das Rollenkonzept lassen sich Modelle unterschiedlicher Schutzprofile nach dem Common Criteria CIMC (Certificate Issuing and Management Components) erstellen, die die meisten PKI-Anbieter auch unterstützen. Unterschieden wird im höchsten Schutzprofil zwischen Administratoren der CA, Zertifikatsverwalter, Auditoren und Sicherungsoperatoren. Wichtig hierbei ist, dass eine Person niemals mehr als eine Rolle einnehmen darf.

Darüber hinaus sind weitere Faktoren für den sicheren und störungsfreien Betrieb einer eigenen PKI zu berücksichtigen:

- Ablaufdaten wichtiger Zertifikate der Hierarchie
- Ablaufdaten der CRLs
- Verwaltung der Zertifikatsvorlagen
- Backup- und Recovery-Planung
- Berechtigungen auf den Servern und Backups
- Zugriff auf die Infrastruktur (insbesondere virtualisierte Instanzen)
- Revisionssichere Auditierung aller Aktionen innerhalb der PKI-Umgebung (SIEM-Integration)

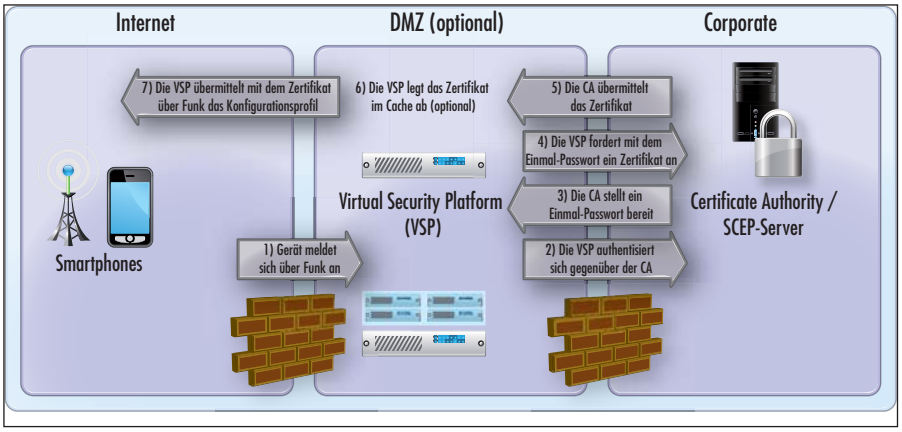


Bild 2: Bereitstellung von Zertifikaten für iOS-Devices mittels SCEP

Option Outsourcing

Angesichts der vordergründig doch recht hoch erscheinenden Hürden ist eine mögliche Alternative zum Betrieb der eigenen PKI die Nutzung von SaaS-Angeboten, auch Managed-PKI genannt. Hierbei übernimmt ein Trustcenter den Betrieb der PKI, wobei die Kosten für die Implementierung, Software, Hardware und Betrieb der Komponenten einer eigenen Installation gegen eine Gebühr pro ausgestelltem Zertifikat gegengerechnet werden müssen.

Einen Vorteil bieten diese Outsourcing-Lösungen in Bezug auf das Zertifikat der ausstellenden PKI. Dieses ist meist aufgrund der in typischen Endgeräten und Softwarepaketen enthaltenen Root-CAs als vertrauenswürdig anerkannt, was für die Zertifikate einer eigenen CA nicht ohne weiteres möglich ist. In der Realität finden sich in Unternehmen häufig hybride Modelle, die sowohl eine selbst betriebene PKI – beispielsweise für die Nutzung von Smartcards – vorsehen sowie eine zusätzlich implementierte Sub-CA eines Managed-PKI Anbieters zur Nutzung in einer Gateway-basierten E-Mail-Verschlüsselungslösung.

Hinsichtlich der Flexibilität ist die SaaS-Variante der eigenen PKI deutlich unterlegen. Dies gilt zum Beispiel für die Auswahl von 3rd-Party Softwarekomponenten (CMS, Card Management System), individuelle Zertifikatsvorlagen oder Auto-Enrollment-Verfahren in Microsoft-Umgebungen. Der gravierende Nachteil jedoch ist die Auslagerung des einzigen Kapitals einer PKI –Vertrauen – zu einem externen Anbieter.

Anwendungsfälle im Detail

Abschließend betrachten wir anhand zweier Szenarien den Einsatz von PKI in der Praxis. Diese beleuchten beispielhaft den Nutzen von PKI für ausgewählte Dienste.

Smartcardanmeldung an Webservices

Die Verwendung von Passwörtern zur Anmeldung an Rechnersystemen oder Webservices ist immer noch der Standard in den meisten Unternehmen. Dabei sind die Unzulänglichkeiten dieses Anmeldeverfahrens wie schwache Passwörter, die einfache Weitergabe, häufige Wiederverwendung (auch im privaten Bereich), fehlender Komfort für den Anwender und mangelhafte Unterstützung von SSO (Single Sign-On) triftige Gründe für eine Umstellung auf Smartcard-basierende Anmeldung unter Verwendung von Zertifikaten.

Neben gängigen Szenarien wie Anmeldung an Arbeitsstationen oder Terminaldiensten spielen auch dezentrale Authentifizierungsverfahren eine immer größere Rolle. Dies wird durch die rasant wachsende Zahl an Webservices weiterhin zu-

nehmen und es gibt mit ticketbasierenden SSO-Lösungen eine komfortable und zugleich auch sichere Möglichkeit, die Anmeldung durchzuführen. Verfahren wie OpenID oder SAML v2 können vereinfacht dargestellt anwenderseitig ein Smartcard-gespeichertes Zertifikat zur Authentifizierung des Benutzers anfordern und treten dann als sogenannter Identity Provider (IdP) gegenüber dem eigentlichen Webservice (Service Provider) auf.

SCEP für mobile Geräte

In zunehmendem Maße ist die Bereitstellung von Zertifikaten für mobile Systeme erforderlich, die Zugriff auf Unternehmensressourcen erhalten sollen. Dies können Zertifikate sein, die im Umfeld einer Anmeldung am WLAN mittels 802.1x oder zur Authentifizierung eines Gerätes innerhalb von RAS verwendet werden. Diese Zertifikate lassen sich zwar manuell erstellen und auf entsprechende Geräte importieren, doch ist die automatische Bereitstellung mittels SCEP deutlich komfortabler und skalierbarer.

In Bild 2 sehen Sie die Integration von Apple iOS-basierten Systemen: Das Endgerät ist mittels eines Konfigurationsprofils so eingerichtet worden, dass es bei einer SCEP-Registrierungsstelle ein Zertifikat mit vordefinierten Eigenschaften anfragt. Dies kann entweder ein SCEP-Proxy sein (beispielsweise eine Mobile Device Management Instanz) oder der SCEP-Service der PKI. In diesem Beispiel generiert der SCEP-Proxy ein Schlüsselpaar und leitet daraus den CSR ab, der nach Authentifizierung mit einer Challenge von der CA signiert wird.

Anschließend erfolgen das Packaging mit dem signierten Zertifikat und die Übertragung zum Endgerät. Hier kann das Zertifikat dann zum Beispiel zur Authentifizierung im WLAN genutzt werden. Ein sicherer Remote-Zugriff über ein SSL-VPN nur anhand dieses Zertifikates ist damit noch nicht gewährleistet, dazu wird neben dem derart vorkonfigurierten Device (erster Faktor) noch ein zweiter Faktor (Passwort, OTP-Code) empfohlen.

Ein solches Setup ist bei einer bestehenden PKI meist recht problemlos bereitzustellen und beweist, dass die zunehmende Mobilisierung sehr gut mit einer Zertifizierungsstelle abgesichert werden kann.

Fazit

Public Key Infrastrukturen werden durch die enorme Zunahme an zertifikatsgestützten Verfahren in den letzten Jahren immer wichtiger. Die Treiber sind hier vor allem die Authentifizierung von Geräten in unterschiedlichsten Zugriffsverfahren auf Netzwerkdiensten sowie Web- und Cloud-Diensten. Damit nicht für einzelne Anwendungsszenarien Insellösungen geschaffen werden, lohnt es sich für ein Unternehmen in die Planung einer PKI zu investieren und somit eine flexible sowie sichere Struktur zu schaffen, die dann sukzessive für zusätzliche Authentifizierungsverfahren erweitert werden kann. *(jp)*

Dr. Ralf Stodt ist Executive Solution Manager, CISSP bei der Integralis Deutschland GmbH.

Vier Open Source-Storage-Systeme im Überblick

Self Storage

von David Breitung


Quelle: Maren Wischnewski - 123RF

Storage muss flexibel erweiterbar und verwaltbar sein. Doch im Gegensatz dazu steht ein in den letzten Jahren deutlich gestiegener Kostendruck, der IT-Betreiber zu einer effizienten und kostengünstigen Bereitstellung von Ressourcen zwingt. Die Lösung sind Unified Storage-Systeme, die alle Speicherressourcen an einem zentralen Punkt zusammenführen und so eine effiziente Ablage und flexible Verteilung ermöglichen. IT-Administrator stellt vier interessante Open Source-Projekte vor.

Open Source-Anwender müssen nicht auf die zentralen Funktionen eines Unified Storage verzichten. Datenspiegelungen, Snapshot-Sicherungen, Deduplizierung – die Liste der Features, die aus Communities hervorgegangen sind, ist lang. Und meist sind diese Lösungen, wie zum Beispiel die Datenspiegelung "DRBD", bereits seit vielen Jahren praxiserprobt und so auch im Unternehmensumfeld einsetzbar. Allerdings sind zur Abdeckung einer Anforderung mit Open Source häufig mehrere Tools notwendig, die eng miteinander verzahnt werden müssen. Um die Komplexität eines derartigen Konstrukts zu reduzieren und einen stabilen Betrieb zu gewährleisten, empfiehlt sich der Einsatz eines Management Frameworks. Hierüber können die administrativen Tätigkeiten in einem zentralen Punkt zusammengeführt und vereinheitlicht werden. Die Zusammenführung der breit aufgestellten Werkzeugpalette wandelt das System in eine Unified Storage Toolbox. In den vergangenen Jahren sind zu diesem Zweck diverse Projekte entstanden, die trotz des ähnlichen Funktionsumfangs zum Teil sehr unterschiedliche Ansätze verfolgen. Bei der Wahl der passenden Lösung empfiehlt sich daher, neben den Funktionen auch die Gesamtkonzeption und Ausrichtung zu vergleichen.

FreeNAS

FreeNAS [1] ist ein auf FreeBSD aufsetzendes Storage Framework. Durch die BSD-Basis hebt sich FreeNAS von anderen Projekten in diesem Segment ab und kann nativ auf Oracles Dateisystem ZFS aufsetzen. Ursprünglich als reines NAS-System ausgerichtet, unterstützt FreeNAS nun neben Standardprotokollen wie NFS, CIFS, FTP oder AFP mit iSCSI auch ein SAN-basiertes Protokoll. Der Einsatz von ZFS ermöglicht die einfache und schnelle Sicherung der Daten, zum Beispiel durch Snapshots auf Dateisystemebene oder die Bereitstellung von virtuellen RAIDs. Auch eine Spiegelung von einzelnen Speicherbereichen auf ein zweites System ist mit den Bordmitteln von FreeNAS möglich.

Ein Hochverfügbarkeitscluster mit einer automatischen Host-Umschaltung im Fehlerfall kann allerdings nicht konfiguriert werden. Das schützt vor Datenverlust, garantiert aber nicht die Verfügbarkeit der bereitgestellten Dienste. Ein professioneller Support wird von iXsystems angeboten, die mit TrueNAS eine getrennte – auf FreeNAS aufsetzende – Distribution betreuen. Durch die Nähe der beiden Projekte kann iXsystems in eingeschränkter Form auch FreeNAS-Anwender betreuen.

openFiler

Das Projekt openFiler [2] basiert auf der Linux-Metadistribution rPath und kann als ISO-Datei frei heruntergeladen werden. Wie bei allen Open Source Storage-Projekten erfolgt die Installation auf einem beliebigen Standard-Server. Nach der Basisinstallation werden die Funktionen über eine Weboberfläche konfiguriert. Ebenso wie FreeNAS war auch openFiler ursprünglich als reiner Network Attached Storage ausgelegt. Durch die Business-orientierte Ausrichtung des Projektes wurde in den neueren Versionen von openFiler mit iSCSI auch ein SAN-basiertes Protokoll ergänzt. Zusätzlich kann die Unterstützung des Fibre Channel-Protokolls nachinstalliert werden. Diese kostenpflichtige Erweiterung ist jedoch in der Open Source-Edition nicht enthalten. Durch die Integration einer blockbasierten Datenspiegelung auf Basis von DRBD, die um ein automatisches Host-Failover erweitert werden kann, stellt openFiler die Speicherbereiche bei Bedarf auch mit einer erhöhten Verfügbarkeit bereit. In Verbindung mit dem angebotenen professionellen Support, der über unterschiedlich umfangreiche Wartungsverträge buchbar ist, eignet sich openFiler nicht nur für den Einsatz in Test- und Entwicklungsumgebungen, sondern kann auch bei der Konzeption von produktiven Systemen berücksichtigt werden.

openmediavault

openmediavault [3], ein weiteres Linux-basiertes Storage Framework, wurde im Oktober 2011 veröffentlicht. Trotz des noch jungen Alters kann openmediavault bereits jetzt mit breit aufgestellten Funktionen glänzen. Grund ist die lange Entwicklungszeit vor Herausgabe der ersten Version, begünstigt durch die Erfahrung des Projektinitiators, der bereits bei der Gründung von

FreeNAS beteiligt war. Auch openmediavault unterstützt die gängigen NAS-Protokolle und führt sie in einer intuitiven Web-Oberfläche auf Basis von ExtJS zusammen. Der Weg für weitere Funktionen ist von Haus aus geebnet, da zusätzliche Erweiterungen als Module eingebunden werden können. Das erleichtert die Weiterentwicklung durch die Community und die Einrichtung für den Anwender.

Allerdings orientiert sich openmediavault aktuell eher an den Anforderungen eines Heimgebrauchs und zielt weniger auf den Einsatz im geschäftlichen Umfeld ab. So wird für openmediavault bislang kein professioneller Support angeboten. Auch auf die hochverfügbare Bereitstellung von Speicher muss in der aktuellen Version verzichtet werden. Zwar ist mit rSync eine dateibasierte Replikation von Daten möglich, eine synchrone Spiegelung oder gar ein automatisches Failover zwischen mehreren Instanzen ist bislang aber nicht integriert.

openATTIC

Mit openATTIC [4] entstand erst vor wenigen Monaten ein weiteres quelloffenes Storage-Projekt. Ähnlich wie openmediavault wurde auch openATTIC erst nach einer mehrjährigen Entwicklungsphase veröffentlicht. Das Projekt bietet dadurch einen großen Funktionsumfang, der dem der anderen Projekte gleicht.

Der Schwerpunkt liegt allerdings auf dem Einsatz in Rechenzentren und hochverfügbaren Umgebungen. Herzstück des Systems bildet eine offene API auf Basis von XMLRPC, über die jegliche Funktion auf einem standardisierten Weg angesteuert werden kann. Dadurch integriert sich die Storage-Landschaft flexibel in angrenzende Lösungen wie Provisioning- oder auch Monitoring-Systeme. Des Weiteren ist über diese API die Automatisierung von Backup-Prozessen möglich – wie etwa das Erstellen konsistenter Snapshots von Datenbanken und virtuellen Umgebungen. Integriert sind auch die synchrone Spiegelung von Daten und ein automatischer Failover, wodurch auch die Anforderungen von hochverfügbaren Produktivsystemen abgedeckt werden. Auch in der Distribution unterscheidet sich openATTIC von vergleichbaren Frameworks. Die Entwickler setzen nicht auf vorgefertigte Image-Dateien, sondern liefern openATTIC als Installationspaket für unterschiedliche Linux-Distributionen aus. Die Hardware-Kompatibilität ist dadurch deutlich größer. Support für openATTIC bietet der Open Source-Dienstleister it-novum an.

Professionelle Storage-Systeme

Bei Betrachtung der Storage Management-Lösungen im Open Source-Umfeld zeigt sich, dass die reine Bereitstellung von Speicherplatz über unterschiedliche Protokolle eine Mindestanforderung darstellt, die jedes der aufgeführten Projekte abdecken kann. Beim Einsatz in Business-Szenarios sind die Anforderungen jedoch deutlich höher. Hier rücken Funktionen wie Datenspiegelung und automatisierte Hochverfügbarkeit in den Mittelpunkt. Da diese Funktionen bereits als fester Bestandteil in openFiler und openATTIC integriert sind, sind diese Projekte gut für den Business-Einsatz vorbereitet. Auch FreeNAS bietet durch die Integration von ZFS und der damit verbundenen Deduplizierung eine sehr effiziente Speicherverwaltung. Die eingeschränkte Hochverfügbarkeit bleibt in diesem Punkt jedoch eine große Schwachstelle.

Die modularen Architekturen von openATTIC und openmediavault bieten größtmögliche Flexibilität und Erweiterbarkeit. Die im Open Source-Storagebereich einzigartige zentrale API von openATTIC bietet große Erweiterungsmöglichkeiten. Bei der Einführung eines Open Source-Storage-Systems sollte deshalb im Vorfeld der Verwendungszweck genauestens definiert werden. Die Projekte ähneln sich zwar auf den ersten Blick, unterscheiden sich aber sehr stark in ihrer Ausrichtung und den damit verbundenen Funktionen. *(dr)*

David Breitung ist Head of Business Critical Computing bei it-novum GmbH und Mitgründer des Open Source-Projekts openATTIC.

Storage-Systeme im Vergleich

	FreeNAS	openFiler	openmediavault	openATTIC
Verfügbarkeit				
Lizenz	BSD	GPLv2	GPLv3	GPLv2
Bereitstellung	CD-Image	CD-Image	CD-Image	deb./.rpm Pakete
Unterstützte Protokolle				
NFS	✓	✓	✓	✓
CIFS/Samba	✓	✓	✓	✓
AFP	✓	–	✓	–
FTP	✓	✓	✓	✓
HTTP	✓	✓	–	✓
iSCSI	✓	✓	✓	✓
Fibre Channel	–	Kostenpflichtig	–	In Entwicklung
Ausfallsicherheit				
Datei-Replikation	✓	✓	✓	✓
Block-Spiegelung	–	✓	–	✓
Automatisches Failover	–	✓	–	✓
Angebotener Support				
Wartungsverträge	✓	✓	–	✓
24x7 Support	–	✓	–	✓

Link-Codes

[1] FreeNAS-Projektseite
C5W11

[2] openFiler-Projektseite
C5W12

[3] openmediavault-Projektseite
C5W13

[4] openATTIC-Projektseite
C5W14

Als Opa Admin war: IBM 726

Evergreen

von John Pardey

Wir haben in unserer "Als Opa Admin war"-Rubrik in den vergangenen Monaten zahlreiche Technologien und Produkte betrachtet, die mittlerweile längst ausgedient haben. Und doch gibt es in der Informationstechnologie einen echten Evergreen, dem wir uns heute zuwenden wollen: das Magnetspeicherband. Urvater aller Bandspeicher ist (einmal mehr) die IBM, die 1952 mit der "IBM 726" das erste Gerät für das Tape-Backup vorstellte.

Allen Paradigmenwechseln trotzend stellt diese Technologie auch 60 Jahre nach ihrer Einführung in vielen Unternehmen das Rückgrat der Backup-Infrastruktur bereit. Zwar veränderte sich der Standard für Magnetbandspeicher in dieser Zeit einige Mal und mündet in den aktuellen LTO 5-Standard (mit LTO 6 am Horizont), doch die grundlegende Herangehensweise blieb gleich. Und als Medium zur preisgünstigen Langzeitarchivierung ohne Stromverbrauch gehört Tape noch immer zu den Speichertechnologien professioneller Unternehmens-IT. Doch wie wir gleich sehen werden, war die ursprüngliche Intention der Magnetbandtechnologie weder das Backup noch die Archivierung von Daten.

Abschied von der Lochkarte

Die Ursprünge der Magnetbandtechnologie gehen zurück in die 1930er Jahre mit der Erfindung des Tonbandes zur Musikaufzeichnung in Deutschland. Mitte der 1950er Jahre wurden bereits Großrechner eingesetzt, die simple Kalkulationen in Massen bearbeiten konnten. Diese Mainframes wurden damals mit Programmen in Form von Lochkarten versorgt. Da die Mainframes in speziell klimatisierten Räumen standen, befanden sich die Operator-Terminals zum Einlesen der Lochkarten meist außerhalb dieser Räume.

Aus diesem Grund wurde Mitte der 1960er Jahre ein Weg gesucht, die Lochkarten vorab einzulesen und gesammelt dem Mainframe zuzuführen. Dies war die Geburtsstunde der Magnetbandtechnologie in der IT. An den Operator-Terminals wurden zukünftig die Lochkarten auf ein Magnetband eingelesen und dann zum Mainframe gebracht, der anschließend die Abarbeitung der Programme begann.

720 Meter Daten

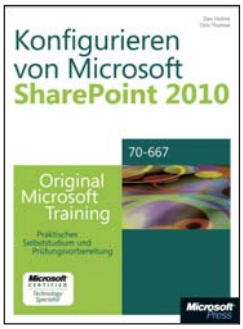
IBM stellte die 726 im Jahr 1952 der Öffentlichkeit vor und präsentierte somit die erste externe Speichereinheit in der Geschichte der IT. Das sehr große Gerät verfügte über eine Speicherkapazität von 1,44 MByte auf einem 12-Zoll-Rollenband mit 720 Meter Länge. IBMs Bandlaufwerk war in der Lage, 7.500 Zeichen pro Sekunde zu lesen oder zu speichern.

Die Speicherung auf dem Magnetband erfolgte in sieben Spuren: sechs davon nahmen je ein Bit auf, während die siebte für das Paritätsbit diente. Dabei ließen sich die Banddaten (im Unterschied etwa zu heutigen Festplatten) nicht frei schreiben und lesen, sondern ausschließlich linear. Im schlimmsten Fall dauerte der Zugriff auf einen einzelnen Datensatz zwei Minuten – so lange brauchte die 726, um die 720 Meter Band komplett zu spulen.

Heute kann ein LTO 5-Laufwerk bis zu 3,2 TByte komprimierte Daten sichern bei einer Lesegeschwindigkeit von bis zu 360 MBit/s. Doch leistungsfähiger als die Lochkarten war die IBM 726 allemal, setzte sich daher durch und bildet die Grundlage einer erfolgreichen Klasse an Speichergeräten.

1,44 MByte Speicher auf dem schrankgroßen Magnetbandgerät IBM 726 nahmen eine Menge Raum im Rechenzentrum ein

Konfigurieren von Microsoft SharePoint 2010



In ihrem Buch "Konfigurieren von Microsoft SharePoint 2010" widmen sich die Autoren dem Aufbau einer komplexen SharePoint-Umgebung. Ihr Ziel: den zertifizierungswilligen Leser zu einem SharePoint-Experten ausbilden. Voraussetzungen dafür sind jedoch ein solides Grundwissen über die Arbeits- und Funktionsweise von Windows Client- und Server-Netzwerken sowie praktische Erfahrung mit der Konfiguration von SharePoint und dazugehörigen Technologien. Den Einstieg bildet die Erstellung eines SharePoint-Intranets mit der Konfiguration von SharePoint-Farmen und Dienstanwendungen – dem Upgrade widmet sich ein späteres Kapitel des Buches. In den Folgekapiteln befassen sich die Autoren mit der Verwaltung und Automatisierung unter SharePoint. Hierfür behandeln sie sowohl Verwaltungsrollen als auch Werkzeuge und Möglichkeiten der PowerShell.

Bevor sich die Autoren dann dem Schutz und der Verwaltung der Inhalte widmen, zeigen sie die Konfiguration von Webanwendungen auf. Ausführlich beschreiben sie anschließend den Einsatz der SharePoint-Suche. Der zweite Teil des Buches widmet sich dann der Wartung und Steigerung der Leistung, indem der Leser die Möglichkeiten der Hochverfügbarkeit, Sicherung und Überwachung beziehungsweise daraus resultierenden Optimierungsmöglichkeiten erfährt.

Fazit

Wer sich auf die Prüfung zum Examen 70-667 vorbereiten möchte, erhält mit dem vorliegenden Werk über 1.000 Seiten an Informationen, Übungen und prüfungsrelevantem Material. Auf der CD befindet sich unter anderem eine elektronische Prüfungsvorbereitung in englischer Sprache. Dan Holme als anerkannter SharePoint-Experte und MVP sowie sein Co-Autor Alistair Matthews haben ein solides Werk vorgelegt, das es ermöglicht die SharePoint-Technologien im Eigenstudium mit dem selbst festgelegten Tempo zu studieren. Die Lektionen werden zusammengefasst und um eine Lernzielkontrolle ergänzt, was eine eigenständige Überprüfung des Wissensstandes ermöglicht. Erfahrungen (und eine entsprechende SharePoint-Umgebung) werden hierfür jedoch vorausgesetzt – die Inhalte richten sich nicht an reine SharePoint-Einsteiger.

Frank Große

Autoren	Dan Holme, Alistair Matthews
Verlag	Microsoft Press
Preis	79,00 Euro
ISBN	978-3866459670
Bewertung *(max. 10 Punkte)*	**9**

NoSQL

In Anbetracht der steigenden Daten bei Unternehmensanwendungen wurden relationale Datenbanken und später daraus SQL entwickelt. Mit Beginn dieses Jahrhunderts entstanden freie Implementierungen von relationalen, per SQL abfragbaren Datenbanken, wie mySQL oder PostgreSQL. Die neuesten Entwicklungen wenden sich vom Prinzip der relationalen Datenbanken ab und verfolgen alternative Ansätze. Den Einblick hierfür will die Zweitauflage des Buches "NoSQL" geben. In drei Teile gegliedert, beginnen die Autoren zunächst mit der Aufklärung des NoSQL-üblichen Fachjargons, sodass Definitionen wie "Consistent Hashing", "CAP Theorem" oder "Paxos" im weiteren Buchverlauf keine Fragen mehr aufwerfen. Die Autoren verfolgen bei den Erklärungen eine gut verständliche Schreibweise jenseits von akademischer Abstraktion. Darauf aufbauend folgen im Hauptteil repräsentative Datenbanklösungen mit einer kurzen Einführung und deren spezifischer Charakteristik. Dies untergliedert sich in folgende Datenbanken: Wide Column Stores, Document Stores, Key Value und Graph. Neben kurzen Installationshinweisen zeigen die Autoren in einer Kurzzusammenfassung die Vor- und Nachteile auf.

In der Neuauflage sind drei Kapitel hinzugekommen: REST für NoSQL, Membase und OrientDB, aber auch die bemängelten Nachlässigkeiten im Lektorat wurden weitestgehend behoben. Die Neuerungen in den Entwicklungen der Datenbanken haben ebenso Einzug gefunden, wie die explosive Ausdehnung des Bereiches der Graph Datenbanken. Über die Tendenzen im Bereich newSQL wird der Leser ebenso informiert, wenngleich die neuesten Entwicklung hier nach einer eigenständigen Publikation verlangen.

Fazit

Auf 410 Seiten haben sich die Autoren der Aufgabe gestellt, Basiswissen und einen Überblick über aktuelle Systeme nachvollziehbar zu vermitteln. Das ist dem Team weitestgehend gut gelungen. Voraussetzung bleibt jedoch, dass die Leser bereits Erfahrung im Umgang mit SQL vorweisen können. Der Begriff "NoSQL" ist dabei nicht dahingehend zu interpretieren, dass die Systeme keine SQL- oder QQL-Syntax verstehen, sondern darf durchaus als "Not Only SQL" verstanden werden.

Das Buch beleuchtet innerhalb komplexer Architekturen den Einsatz großer Datenbestände unter der Notwendigkeit von Faktoren wie Verteilung, Offline-Verfügbarkeit und Cloud. Dabei werden systematisch Hintergründe, Möglichkeiten und derzeitige Produktlösungen aufgeführt, ohne mögliche Risiken zu verschweigen. Wer hingegen detaillierte Produktdokumentationen sucht, wird im Internet fündiger. *Frank Große*

Autoren	Stefan Edlich, Achim Friedland u.a.
Verlag	Hanser
Preis	29,00 Euro
ISBN	978-3446427532
Bewertung *(max. 10 Punkte)*	**7**

http://serversupportforum.de

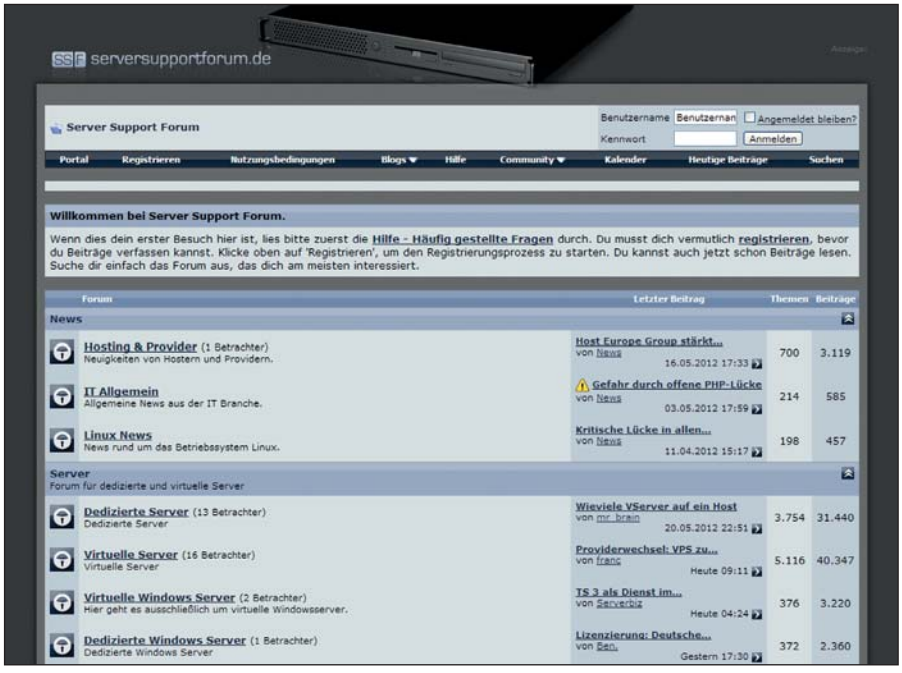
Gut besuchte Server-Gemeinschaft

Egal, ob virtuell oder physikalisch, Windows oder Unix: Server gehören für jeden Administrator zur IT-Grundausstattung. So stieg die Zahl der in Deutschland betriebenen Server laut Bitkom zwischen 2008 und 2011 um sieben Prozent auf gut 2,3 Millionen an. Besonders die großen Rechenzentren haben ordentlich zugelegt. Die Zahl der größeren und mittleren Rechenzentren mit mindestens 500 physikalischen Servern sei demnach um 15 Prozent auf etwa 500 gestiegen. Kleinere Rechenzentren befinden sich dagegen weiter auf dem Rückzug.

So breit wie die Server-Welt selbst ist auch das "Server Support Forum" aufgestellt. Über 50 verschiedene Foren in elf Kategorien weist das deutschsprachige Portal auf. Eine beachtliche Menge. An Usern mangelt es der Site ebenfalls nicht. Laut dem Betreiber Thorsten Neckel tummeln sich rund 20.000 Nutzer auf dem Forum. Dementsprechend rege ist auch der Austausch untereinander. Die monatlichen Besuche liegen bei immerhin rund 300.000. Auf insgesamt knapp 285.000 Beiträge brachten es die Mitglieder zum Zeitpunkt dieses Artikels denn auch. An der Verteilung der Threads lässt sich klar erkennen, wo die User der Schuh am meisten drückt: Themen wie virtuelle Server, dedizierte Server, E-Maildienste sowie die Webserver-Software "Plesk" finden im Forum den meisten Anklang.

Die thematische Bandbreite reicht von dedizierten Servern über virtuelle Server hin zu den verschiedensten Serverdiensten. Der Ton in den Foren ist freundlich und professionell. Meist liegt noch am selben Tag eine Antwort beziehungsweise ein Lösungsversuch für das geschilderte Problem vor. Sowohl die Fragen als auch die Antworten bewegen sich auf einem sehr technischen Niveau, was den hilfesuchenden Admin freuen dürfte – abgesehen von der Tatsache, dass die Forensprache Deutsch ist.

Doch abgesehen von dem umfangreichen Forum hat die Seite noch mehr zu bieten. Tagesaktuelle Nachrichten finden die Besucher auf der Startseite. Ferner gibt es diverse "Interessensgemeinschaften", zu denen sich die Community-Mitglieder zusammenschließen können. Im Vergleich zu den zahlreichen angemeldeten Nutzern scheint sich das Interesse hier jedoch eher in Grenzen zu halten. *(dr)*



Das "Server Support Forum" bietet Hilfe und eine Community rund um Server

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

Mobile Sicherheit durch Trusted Platform Computing

Viele der in deutschen Unternehmen eingesetzten mobilen Geräte werden auch privat genutzt. BYOD erhöht allerdings die Gefahr für sensible Firmendaten. Mit dem von der Trusted Computing Group entwickelten Mobile Trusted Module, einer Hardware-basierten Sicherheitslösung, lassen sich Smartphones und Tablet-PCs gegen Zugriffe von außen schützen. Lesen Sie in unserem Fachartikel im Web, wie das System die Security-Funktionen direkt in die Hardware integriert und damit unabhängig vom jeweiligen Nutzer macht.
Link-Code: C7W51

Anwenderbericht: Clientmanagement bei Freudenberg NOK Mechatronics

Müssen bei der Automobilfertigung Hightech-Bauteile in engen Räumen wie in Außenspiegeln oder im Dachhimmel untergebracht werden, schlägt die Stunde von Freudenberg NOK Mechatronics. Bei der Administration der rund 250 PC-Arbeitsplätze des Unternehmens bereitete der Aufwand für die Integration von Treibern und Software in das damals genutzte Clientmanagementsystem immer größere Sorgen. Lesen Sie in unserem Anwenderbericht, wie es gelang, die Verteilung von Treibern und die Paketierung von Software in einem Viertel der ursprünglich benötigten Zeit umzusetzen.
Link-Code: C7W52

Last- und Performance-Tests optimal durchführen

Ähnlich wie beim Tuning von Motoren kommt es bei Hardware-Installationen darauf an, dass die einzelnen Komponenten optimal aufeinander abgestimmt sind. Hier setzen Last- und Performance-Tests an: Sie prüfen, ob das Zusammenspiel unter den gewünschten Bedingungen klappt, decken frühzeitig Risiken auf und geben Aufschluss über vorhandene Kapazitäten sowie das Systemverhalten in kritischen Situationen. IT-Administrator erläutert auf seiner Webseite, worauf es bei Last- und Performancetests ankommt.
Link-Code: C7W53

Anwenderbericht: Voice-over-IP-WLAN-Telefonie bei avocis

Für Kommunikationsdienstleister ist der reibungslose Kontakt zum Kunden ein essenzielles Qualitätsmerkmal – so auch für die avocis Gruppe. Das Unternehmen setzt dazu auf digitale statt auf klassische Telefonie, sprich Voice-over-IP-WLAN-Telefonie. Um die Vorteile dieser Technologie nicht mit einer geringen Übertragungsqualität und Unterbrechungen zu bezahlen, entschieden sich die Verantwortlichen für die Umstrukturierung ihres Netzwerks in ein virtuelles WLAN. Lesen Sie im Online-Anwenderbericht, ob und wie dies geklappt hat.
Link-Code: C7W54

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

»Anwender sind eine große Gefahrenquelle«

Oliver Schumacher administriert bei arvato Systems, einer Tochter des Bertelsmann-Konzerns, als Leiter des Administratoren-Teams die dortigen Windows-Server. Das Unternehmen betreut die interne IT des Konzerns, bietet aber auch Dienstleistungen für externe Kunden an. Ein Knackpunkt in der IT ist – wie bei den meisten Unternehmen – der Umgang mit mobilen Endgeräten.

Herr Schumacher, warum würden Sie einem jungen Menschen raten, Administrator zu werden?

Wer Technik-affin ist und Spaß am Umgang mit der IT sowie mit Menschen hat, findet eine abwechslungsreiche Aufgabe. Der Beruf ist in meinen Augen unglaublich interessant und vielseitig.

Warum sind Sie IT-Administrator geworden?

Die IT hat mich schon in meiner Jugend interessiert. Ich habe mit dem C64 experimentiert und früh erste kleinere Programme geschrieben. Informationstechnologie ist für mich eine spannende Sache, die durch die permanente Weiterentwicklung nie langweilig wird.

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

Neue Projekte, Herausforderungen und Aufgaben machen den Alltag des Administrators spannend und lassen keine Routine aufkommen. Die Weiterentwicklung von Systemen und Technologien erfordert ein stetiges Mitdenken – das macht den Alltag lebendig. Weniger schön finde ich die Anforderungen einiger User, die manchmal wenig durchdachte, kaum realisierbare Wünsche haben, die wir dann noch innerhalb kürzester Zeit umsetzen sollen.

Wie sichern Sie im Unternehmen Daten auf mobilen Geräten?

Sämtliche mobile Endgeräte werden verschlüsselt, so dass niemand Zugriff auf die Daten hat, falls ein Gerät gestohlen wird oder verloren geht. Darüber hinaus gibt es genaue Anweisungen dafür, welche Daten lokal abgespeichert werden dürfen. Alle relevanten Informationen sind zentral im Netzwerk gesichert. Darauf greifen die mobilen Mitarbeiter über ein gesichertes VPN zu. Für die Sicherung von Endgeräten und Servern nutzen wir OfficeScan von Trend Micro.

Wie gehen Sie mit BYOD-Geräten im Netzwerk um?

Interne Mitarbeiter dürfen im Firmennetz derzeit keine Privatgeräte nutzen. Kunden können mit einem Notebook in einem separaten WLAN arbeiten, haben aber keinen Zugriff auf das Firmennetz.

Worin sehen Sie das größte Sicherheitsrisiko für Endgeräte?

Der Anwender ist immer noch die größte Gefahrenquelle. Das Anklicken dubioser Internet-Seiten sowie unbedachte Downloads bereiten die größten Probleme.

Was bereitet Ihnen bei der IT-Sicherheit die meisten Kopfschmerzen?

Schwierig ist es, dass wir Administratoren in der Regel immer nur reagieren können. Proaktiv haben wir kaum Einfluss auf die Sicherheit von Endgeräten und können auf Lücken meist erst reagieren, wenn schon Probleme aufgetaucht sind.

Wird die IT-Sicherheit im IT-Budget berücksichtigt?

Glücklicherweise werden Sicherheitsprobleme heute nicht mehr belächelt, sondern ernst genommen. Das schlägt sich auch im IT-Budget nieder. Die Sicherheit von Daten und Firmeninformationen hat heute einen deutlich höheren Stellenwert als noch vor wenigen Jahren. Und dafür wird inzwischen auch Geld ausgegeben.

Wo sehen Sie die Trends im Bereich Endpoint und mobile Sicherheit?

Hersteller sind aufgefordert, die Sicherheitslücken der gängigen mobilen Endgeräte deutlich schneller zu schließen. Wichtig ist aber auch ein Umdenken der Anwender. Sie müssen sich der Tragweite ihres Handelns bewusster werden. Dazu gehört der sorgfältige Umgang mit mobilen Daten und Anwendungen. Darüber hinaus sollten die User die sozialen Netzwerke bewusster nutzen und sorgfältiger darauf achten, welche Informationen sie darauf verbreiten.

Wenn Sie sich ein beliebiges Tool wünschen könnten, was würde dieses leisten?

Schön wäre ein Verwaltungstool, das auf Knopfdruck alle Informationen über sämtliche User, Komponenten und Endgeräte zentral bereitstellt, ohne dass man in unterschiedlichen Quellen mühsam danach suchen muss.

Geburtstag: 1969
Admin seit: 13 Jahren
Hobbys: Gartenarbeit, Sport

Oliver Schumacher, IT-Administrator

Ausbildung und Tätigkeit

- Informatikstudium im Rahmen der Ausbildung zum Bundeswehr-Offizier
- Dort als Administrator tätig
- Danach verschiedene Anstellungen bei Privatfirmen
- Seit 2009 bei arvato und am Standort München Leiter des Administratoren-Teams

Betreute Umgebung

- Verantwortlich für das Netzwerk und Betreuung der Windows-Server
- Derzeit rund 50 Windows-Server, davon zwei Drittel virtualisiert
- Betreuung der Unix-Server durch ein anderes Team

Welches ist der lustigste Anwenderfehler, der Ihnen untergekommen ist?

Ein Anwender hatte seine persönlichen Einstellungen so verändert, dass er plötzlich mit weißer Schrift auf weißem Hintergrund arbeitete.

Wie finden Sie den nötigen Ausgleich zu Ihrer Arbeit?

Bei der Gartenarbeit sowie bei der Familie und mit Freunden.

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 8/12 erscheint am 30. Juli 2012

Schwerpunktthema:

Infrastruktur & Inventarisierung

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

Der Schwerpunkt unserer Ausgabe im **September** befasst sich mit dem Thema **Collaboration & Unified Communications**. In unseren Tests stellen unter anderem Kerio Connect 7.4 und WinGate 7 ihr Können unter Beweis. Zudem nehmen wir die SharePoint-Administration mit AvePoint DocAve 6 unter die Lupe. In der Praxisrubrik erfahren Sie, wie Sie Unified Communications-Ressourcen administrieren und was die freie SharePoint-Alternative Liferay zu bieten hat.

Als Schwerpunkt im **Oktober** geht es dann um **Server-Sicherheit**.

Im Test: Avocent Data Center Planner 4.0

Im Test: Raritan Power IQ 3.1.1

Workshop: Citrix Receiver und Receiver StoreFront Services

Workshop: DHCP- und DNS-Server ausfallsicher betreiben

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 und CvD*
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, Michael Bock, David Breitung, Thomas Gronenwald, Frank Große, Marc Grote, Jürgen Heyer, Thomas Joos, Martin Kuppinger, Sandro Lucifora, Michael Lüscher, Dr. Holger Reibold, Thorsten Scherf, Dr. Ralf Stodt

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

Es gilt die Anzeigenpreisliste Nr. 9 vom 01.01.2012

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.special-interest.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

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

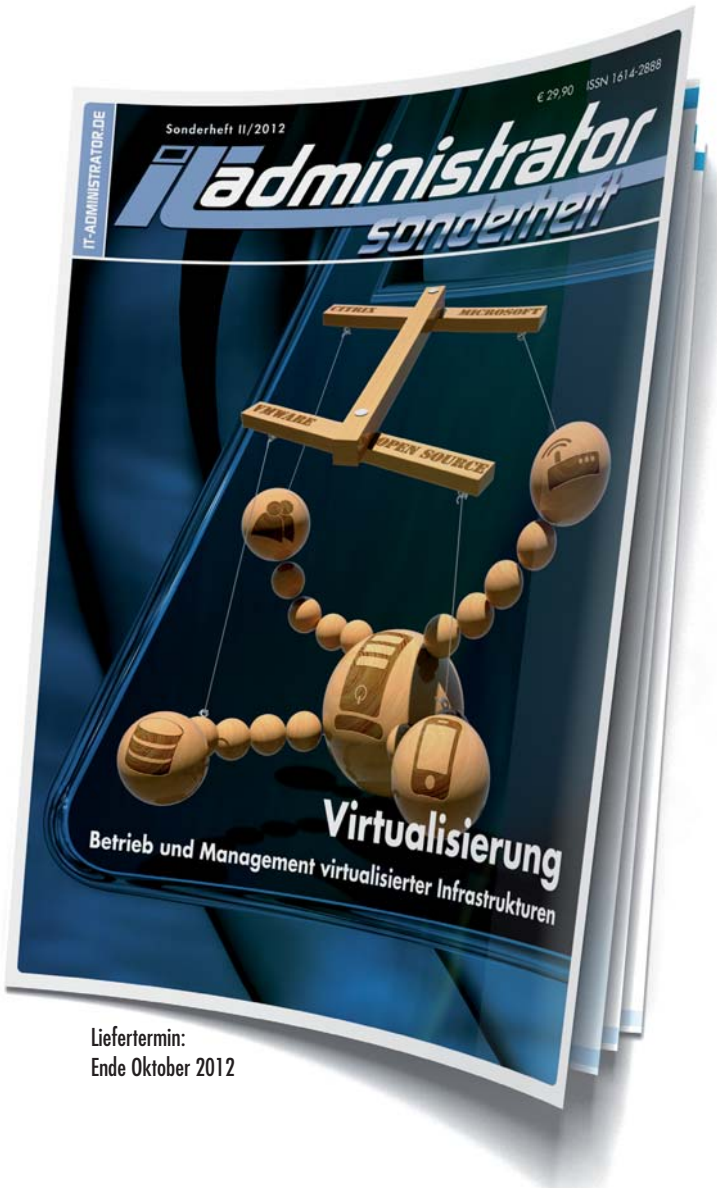
So erreichen Sie die Redaktion
Redaktion IT-Administrator
Heinemann Verlag GmbH
Leopoldstr. 85
80802 München
Tel.: 089/4445408-10
Fax: 089/4445408-99
E-Mail: redaktion@it-administrator.de

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

Dieser Ausgabe liegt eine Gesamtbeilage der Firma transtec bei.



Liefertermin:
Ende Oktober 2012

Bestellen Sie jetzt

das IT-Administrator

Sonderheft II/2012!

180 Seiten Praxis-Know-how rund um das Thema

Virtualisierung

Betrieb und Management virtualisierter Infrastrukturen

zum Abonnenten-Vorzugspreis von*

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft II/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.*

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

iladministrator
Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft II/2012 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft II/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 0712

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

BUILT FOR
THE HUMAN
NETWORK

EIN SERVERSYSTEM, DAS NEUE WEGE BESCHREITET

Wir haben den Markt durch Innovationen grundlegend verändert.
Über 11.000 zufriedene Kunden sprechen eine deutliche Sprache:

80 % verbesserte Produktivität von Administratoren
90 % reduzierte Bereitstellungszeit
40 % verbesserte Anwendungsleistung
30 % gesenkte Infrastrukturkosten

Als zentrale Komponente des Cisco Unified Computing System™ sorgen unsere Server für effiziente und produktivere Betriebsabläufe. Das Cisco UCS besticht durch Integration, Automatisierung, Performance und Skalierbarkeit. Mit Cisco als Partner lassen sich so die Visionen von morgen bereits heute in die Realität umsetzen.
Weitere Informationen erhalten Sie unter cisco.de/servers.

Das Cisco UCS verfügt über einen integrierten Intel® Xeon®-Prozessor der neuesten Generation.