

01/2010

iAdministrator

Das Magazin für professionelle System- und Netzwerkadministration

**Im Test:
Shavlik NetChk Protect 7.1
Mehr als nur Flickschusterei**

Sonderdruck für Prosoft



Im Test: Shavlik NetChk Protect 7.1

Mehr als nur Flickschusterei

von Jürgen Heyer

Ein aktueller Patchstand auf allen PCs und Servern im Unternehmen ist ein unverzichtbarer Schutz gegen die ständigen Wurmattaen und Hackerangriffe. Mit NetChk Protect gehört Shavlik seit Jahren zu den führenden Anbietern für Patchwerkzeuge und verspricht mit der neuen Version 7 noch mehr Flexibilität im Einsatz. So deckt das Programm auch die Funktionen Antivirus sowie Antispy ab und versucht sich zudem beim Asset Management. IT-Administrator hat das Gesamtpaket einmal genau unter die Lupe genommen.

Die Kernkompetenz von Shavlik liegt schon seit Jahren beim Patchmanagement im Windows-Umfeld. Das kommt nicht von ungefähr, denn Shavlik war maßgeblich an der Entwicklung der in Windows integrierten Updateprozesse beteiligt, so dass umfassendes Knowhow vorhanden ist. Mit seinem Produkt NetChk Protect 7.1 (NCP) verfolgt Shavlik mittlerweile mehrere Strategien. So will der Hersteller deutlich mehr Komfort, Umfang und Flexibilität beim Patchen bieten als Microsoft mit seinem kostenlosen WSUS. Außerdem hat Shavlik damit begonnen, weitere aus Client-Sicht wichtige Funktionen zu integrieren, mit dem Ziel, dem Administrator die Arbeit zu erleichtern.

Mit NCP soll der Administrator nur ein Werkzeug und eine zentrale Management-Konsole bedienen müssen, um zu patchen, Viren und Spyware fernzuhalten sowie die Ausstattung der Clients zu inventarisieren. Ein zusätzlicher Vorteil ist, dass statt mehrerer Agenten auf den Endsystemen nur einer notwendig ist, wobei das Patchen sowie das Asset Management alternativ auch ohne Agenten auskommen.

Reibungslose Installation

Die Einrichtung von NCP bereitet keinerlei Probleme. Auch wenn die Ober-



Bild 1: Die Quickstart-Seite erleichtert Assistenten-gesteuert den Einstieg in NetChk Protect

fläche nach wie vor nicht in Deutsch, sondern nur in Englisch verfügbar ist, klappt die Einrichtung auf einem deutschen Windows 2008 Server (64 Bit) auf Anhieb. Erfreulich ist, dass die Setup-Routine alle Systemvoraussetzungen prüft und fehlende Komponenten mitinstalliert sowie konfiguriert. Dazu gehört auch ein MS-SQL Server 2008 Express, sofern nicht ein bereits vorhandener Datenbankserver angegeben wird. Zudem legt NCP mit der Installation einige Standard-Profilen an, um später bei der ersten Benutzung ohne große Vorarbeiten die wichtigsten Analysen durchführen zu können.

Beim ersten Start der Konsole fragt NCP noch einige Einstellungen ab, wie die Daten eventuell verwendeter Proxyserver, einen Standardbenutzer mit Pass-

Leistungsfähige Hardware mit Windows 2003 oder 2008 Server, SQL Server 2005 oder 2008, 2 bis 4 GByte RAM für die Konsole, agentlose Clients unter Windows NT/2000/XP/Vista/2003/2008/7, Offline Images unter ESX Server ab 3.0, VirtualCenter ab 2.0, VMware Server, Workstation und Player, Clients mit Agenten unter Windows 2000 SP4/XP SP2/Vista/2003/2008/7

Systemvoraussetzungen





wort für den Clientzugriff, die IP-Adresse für das Monitoring (falls der Server mehrere Netzwerkkarten hat) sowie Angaben für eine SMTP-Mailzustellung. Abgesehen davon sind einige zusätzliche Konfigurationseinstellungen zu tätigen, allen voran die Auswahl der Sprachversionen, die gepatcht werden sollen.

Weiterhin ist der Lizenzschlüssel einzuspielen, ohne den einige Optionen gesperrt sind. NCP kann auch ohne Lizenz genutzt werden, scannt dann aber nur einen sehr beschränkten Umfang an Microsoft-Produkten. Neben der hier vorgestellten Vollversion gibt es noch eine so genannte Audit-Version, die zwar umfassend scannt, aber keine Verteilung erlaubt und auch keine agentenbasierten Zusatzfunktionen enthält. Sie ist rund ein Drittel günstiger.

In größeren Umgebungen oder auch bei einer Segmentierung eines Unternehmens auf verschiedene Standorte, die womöglich nur über eine langsame WAN-Verbindung kommunizieren können, bietet es sich an, nicht nur mit einem Verteilserver zu arbeiten, sondern wie von NCP unterstützt mehrere Distributions-Server aufzubauen und die Clientdownloads darauf zu verteilen.

Multifunktionale Konsole

Die gesamte Bedienung erfolgt von einer zentralen Managementkonsole aus, was sehr von Vorteil ist. Auch wenn die nach wie vor recht bunte Oberfläche der Konsole einen an sich aufgeräumten Eindruck macht, so ist die Handhabung doch etwas gewöhnungsbedürftig. Immer wieder ist der Anwender versucht, auf irgendwelche Grafiken und Übersichten zu klicken, um mehr zu erfahren, doch dahinter verbergen sich keine zusätzlichen Informationen. Aufgrund der zunehmenden Funktionalität ist die Bedienung im Laufe der Jahre immer komplexer geworden, so dass für eine effiziente Nutzung eine gewisse Einarbeitung erforderlich ist.

Auf der Startseite der Konsole befindet sich rechts ein Fenster, welches den aktuellen Datenstand von NCP anzeigt und auch über die letzten Aktualisierungen berichtet. Das ist wichtig, um zu erkennen, ob die Kommunikation mit den Servern von Shavlik klappt. Die Steuerung erfolgt in erster Linie über eine Fensterleiste mit mehreren Registern auf der linken Seite der Konsole, um zwischen den verschiedenen Ansichten umzuschalten. Bereits bei den ersten Arbeitsschritten halten wir es unbedingt für erforderlich, sich Gedanken über notwendige Gruppierungen zu machen, um festzulegen, welche Clients in welchem Umfang durchsucht und aktualisiert werden sollen. Die Anlage von Maschinengruppen ist in der Regel auch die erste Arbeit bei der Einführung.

Für die Umsetzung der Gruppierung beinhaltet NCP eine fast schon erschlagende Vielzahl an Filter- und Sortierkriterien. So kann ein Administrator das gesamte Netzwerk oder auch nur eine Domäne durchsuchen sowie die Namen aus einer Datei importieren. Weiterhin kann er das Active Directory durchfors-

ten oder einen IP-Bereich vorgeben. Eine Auswahl nach diesen Kriterien kann wiederum nach Servern, Arbeitsstationen, Domänencontrollern, SQL-, IIS-, Einwahl- und Print-Servern gefiltert werden. Zusätzlich lassen sich Gruppen verschachteln. Damit dürfte es kaum Konstellationen geben, die sich mit NCP nicht gruppieren lassen. Zudem ist es ein Leichtes, beispielsweise sowohl anhand der Unternehmensstruktur als auch nach Funktionen zu gliedern und zugleich aus allen Bereichen einige Piloten festzulegen, auf denen die Patches zuerst eingespielt werden.

Sind die Gruppen festgelegt, besteht die nächste Aufgabe in der Anlage von "Patch Scan Templates", also Profilen zur Patchanalyse. Zwei Profile sind hier bereits vorgegeben: Der "Security Patch Scan" sucht nur nach sicherheitskritischen Patches, "WUScan" ermittelt darüber hinaus auch die nicht sicherheitskritischen Patches. Für einen grundlegenden Scan sind diese Profile durchaus geeignet, für eine sinnvolle und effiziente Nutzung ist es allerdings sehr ratsam, sich zusätzlich eigene Tem-

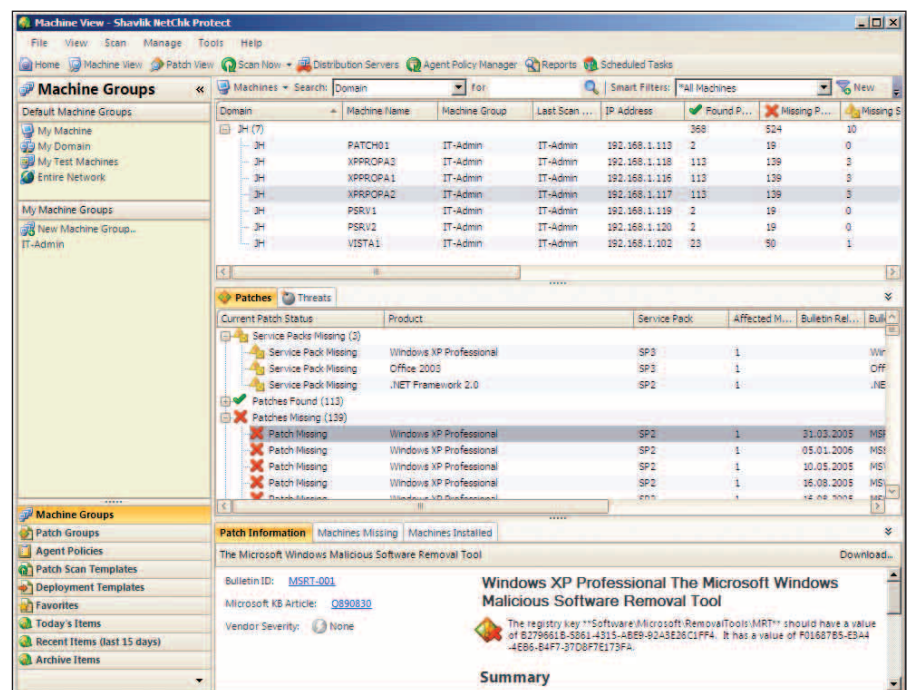


Bild 2: Sehr übersichtlich ist die Anzeige des Patchstandes für einen bestimmten Client, da sowohl die fehlenden als auch die installierten Updates aufgeführt sind



plates mit individuell passenden Parametern zu definieren.

Angesichts der Vielzahl an unterstützten Programmen, die bei der Definition eines Profils angezeigt werden, wird schnell ersichtlich, dass NCP weit mehr als Microsofts WSUS patchen kann. So lassen sich unter anderem auch die Produkte von Adobe, Citrix, Blackberry, Firefox, Google, Realplayer und Skype aktualisieren. Die komplette Übersicht der wirklich umfangreichen Liste ist bei Shavlik einsehbar. Bei der Definition eines Scanprofils lassen sich nun nur einzelne oder auch alle Produkte aufnehmen und dann wieder nach Typ (unter anderem Sicherheitspatches und Tools) sowie Bedrohungsgrad (kritisch, hoch, mittel oder niedrig) filtern.

Die Verteilung erfolgt ebenfalls über Profile, wobei der Administrator den Ablauf sehr granular steuern kann. Dies umfasst beispielsweise die Downloadgeschwindigkeit, aber auch, ob vorher ein SQL-Server oder der IIS heruntergefahren werden soll. Optional können Clients auch vor einer Verteilung gebootet werden. Weiterhin unterstützt NCP die Definition von Abhängigkeiten und möglichen Verzögerungen, wenn ein Anwender angemeldet ist, damit dieser seine Arbeit beenden kann.

Überzeugt hat uns der sehr individuell einstellbare Scheduler. Aufträge können einmalig, aber auch regelmäßig gestartet werden, weiterhin kann der Administrator vorgeben, ob Scanlauf und Patchinstallation zeitlich getrennt oder nacheinander erfolgen sollen und ob ein anschließender Reboot sofort, zu einem bestimmten Datum und/oder Zeit erfolgen soll und ob ein eventuell angemeldeter Benutzer vorher informiert wird, damit dieser den Neustart verschieben oder gar abbrechen kann. Von Vorteil ist, dass sich alle bereits definierten Profile einfach kopieren lassen, um ähnliche Profile zu bilden und dabei etablierte Einstellungen komfortabel zu übernehmen.

Übrigens ist es bei NCP kein Problem, bei Bedarf auch mit mehreren Konsolen zu arbeiten, die beispielsweise bei einem größeren Unternehmen auf unterschiedliche Örtlichkeiten verteilt sind und für die Betreuung der Clients in den jeweiligen Bereichen verwendet werden. Das beschleunigt die Prozesse, da sich unabhängig von verschiedenen Distributionsservern auch die Scannerperformance verbessert, wenn sich so vermeiden lässt, dass über eine langsame Anbindung gearbeitet werden muss. Zusätzliche Konsolen sind allerdings kostenpflichtig zu lizenzieren, während die Anzahl der Distributionsserver keine Rolle spielt.

Einstieg ins Asset Management

Eine ganz neue Funktion in der aktuellen Version 7.1 ist das Asset Management, bei dem NCP die installierte Software sowie die vorhandene Hardware inventarisiert. Ähnlich wie bei den Patchprofilen ist auch für die Inventarisierung ein Profil mit den gewünschten Informationen (BIOS-Version, Netzwerk-, Prozessor- oder Plattendaten und installierte Software) zu definieren. Ein Scanlauf sowie einige Auswertungen zeigen allerdings, dass diese Funktion hinsichtlich der weiteren Verarbeitung noch ausbaufähig ist,

denn die gewonnenen Informationen werden kaum aufbereitet. So kann der Administrator zwar die jeweilige Ausstattung eines Systems betrachten und gesammelte Reports erstellen, weiterführende Funktionen wie eine Lizenzverwaltung sind aber nicht integriert. Auch lassen sich zu einzelnen Assets keine zusätzlichen Informationen hinterlegen.

Nachteilig ist auch, dass alle Anzeigen stets aus Clientsicht erfolgen, also, welche Komponenten auf einem Client installiert sind. Es fehlt aber die Möglichkeit, aus Komponentensicht abzufragen, also, welches Ausstattungsmerkmal, wie eine bestimmte Software oder eine bestimmte CPU, Speicherausstattung und so weiter, auf welchen Clients zu finden ist. Hier besteht noch ein deutliches Optimierungspotential. Beim Patchmanagement sind solche Auswertungen übrigens selbstverständlich möglich: Der Administrator kann nachsehen, welche Updates auf einem Client fehlen, aber ebenso, welcher Patch auf wie vielen beziehungsweise welchen Clients fehlt.

Virtuelle Maschinen offline patchen

Eingangs wurden bereits die umfangreichen Gruppierungsmöglichkeiten für die

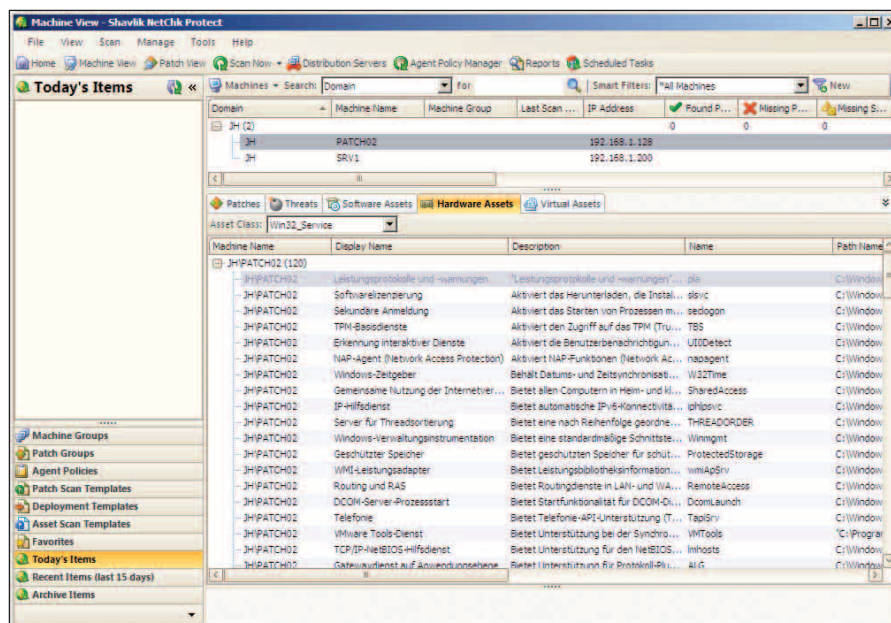


Bild 3: Das Asset Management ist noch auf reine Abfragen beschränkt, die anschließend in Listenform dargestellt werden



zu patchenden Systeme beschrieben, zu denen noch ein besonderes Feature hinzukommt. So verfügt NCP über eine wirklich beeindruckende, umfassende VMware-Unterstützung, denn in eine Gruppe können auch ganze VMware-ESX-Server sowie einzelne virtuelle Maschinen von einem ESX-Server oder auch von einer VMware Workstation-Installation mit aufgenommen werden. Für den Zugriff über einen ESX-Server muss der Administrator entsprechende Anmeldedaten hinterlegen und bei Workstation-Images den genauen Pfad oder auch einen zu durchsuchenden Ordner vorgeben. NCP durchsucht nun den ESX-Server oder auch den angegebenen Pfad nach existierenden VMs und patcht diese. Ein Administrator muss also gar nicht jede VM genau vorgeben, was auch den Vorteil hat, dass bei häufigen Änderungen immer alle gerade existenten virtuellen Maschinen erfasst werden.

Eine Besonderheit ist zudem, dass NCP auch ausgeschaltete virtuelle Images patchen kann. Dazu mountet das Tool die virtuellen Maschinen nacheinander, scannt diese und verteilt auf Wunsch auch die Patches. Letzteres bedeutet, dass es die Installationsdateien in das Image kopiert. Die eigentliche Installation erfolgt dann, wenn die VM das nächste Mal gestartet wird.

Im Test aktualisierten wir ein Image umfassend, insgesamt 96 Updates mit über 800 MByte Gesamtumfang kopierte NCP offline in das Image, um diese nach Starten der VM automatisch zu installieren. In diesem Zuge fiel uns allerdings ein kleinerer Fehler auf. So funktioniert ein Refresh der Anzeige der VMs auf einem in ein Scan-Profil aufgenommenen ESX-Server nicht. Werden auf dem ESX-Server virtuelle Maschinen gelöscht oder ergänzt, muss dieser aus dem Profil entfernt und wieder aufgenommen werden. Der Hersteller will diese Funktion nochmals eingehend prüfen.

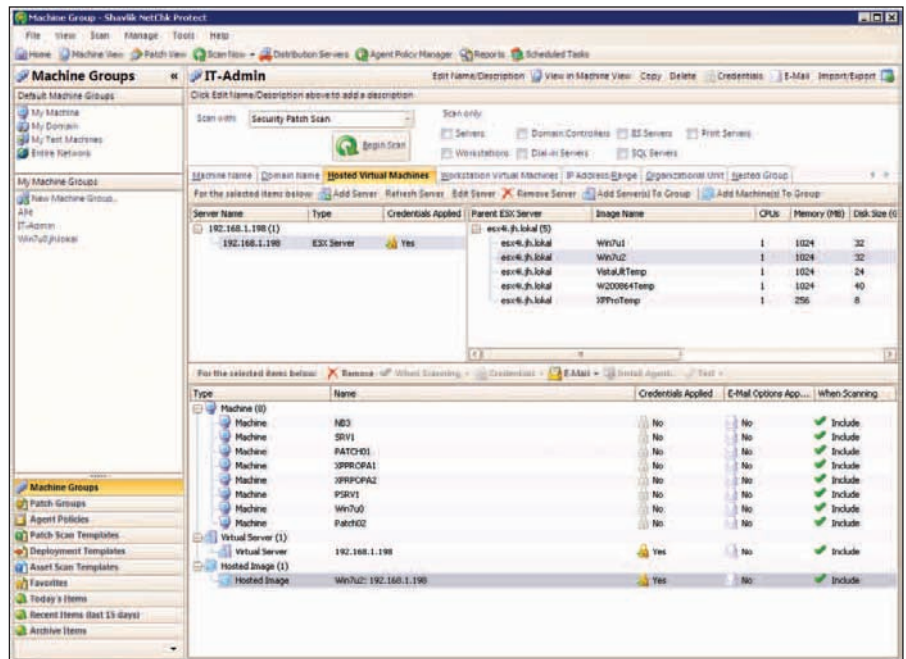


Bild 4: NCP kann alle virtuellen Maschinen eines VMware ESX-Servers einlesen und auch offline, also in ausgeschaltetem Zustand, scannen

Frühzeitige Betriebssystemunterstützung

Zum Testzeitpunkt im Oktober 2009 stand Windows 7 noch nicht in den deutschen Regalen. In NCP ist die Unterstützung aber bereits komplett integriert. Das Gleiche gilt für Windows Server 2008 R2. Auch wenn Unternehmen diese ganz neuen Versionen nicht sofort produktiv einsetzen, ist die frühzeitige Unterstützung dennoch sehr sinnvoll, damit die Patchfunktion bei der Einführung eines neuen Betriebssystems gleich mit evaluiert werden kann. Shavlik ist verständlicherweise auch aus eigenem Interesse an einer sehr zeitnahen Unterstützung interessiert, da sonst einige Kunden gezwungen sein könnten, erst einmal auf Microsofts WSUS zurückzugreifen.

Im Laufe des Tests versuchten wir, verschiedene Clients unter Windows XP Professional, Windows Vista 64 Bit, Windows 7 64 Bit und Windows Server 2008 64 Bit zu patchen, wobei keinerlei Probleme auftraten. Ein Vergleich der Scanergebnisse mit WSUS bei der Suche nach kritischen Patches ergab auch

eine gute Übereinstimmung. Eine Suche nach allen Patches erweist sich letztendlich als nicht exakt vergleichbar, da NCP deutlich mehr installierte Produkte aktualisiert als WSUS. Hier wird der Mehrwert von NCP deutlich sichtbar.

Sofern bei einem Patch eine Deinstallationsmöglichkeit vorgesehen ist, wird diese von NCP unterstützt und kann komfortabel direkt aufgerufen werden. Ob diese Möglichkeit überhaupt besteht, zeigt das Programm übersichtlich an, so dass ein Administrator dies bereits vor einer Installation sieht. Weiterhin zeigt NCP dem Administrator an, ob ein Patch bereits auf die Konsole heruntergeladen wurde oder nicht. Diesbezüglich gibt es zudem die Möglichkeit, entweder in Stundenabständen auf neu erschienene Patches zu prüfen und diese sofort herunterzuladen oder erst dann, wenn ein Scanlauf stattfindet und ein Patch tatsächlich benötigt wird.

Ein weiterer Vorteil ist, dass ein Administrator mit NCP jederzeit in der Lage ist, alle Maschinen im Netz gezielt zu scannen und zu aktualisieren. Von der

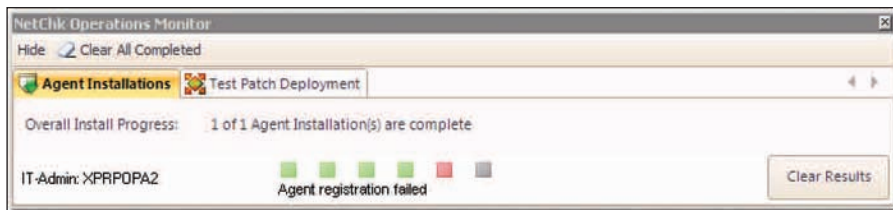


Bild 5: Falls eine Agenteninstallation fehlschlägt, gibt NCP nicht immer einen Grund aus, der eine Fehlersuche erleichtern würde

Konsole aus kann er alle Systeme erreichen und muss nicht warten, bis sich die Systeme wie bei WSUS von sich aus melden (beziehungsweise dieses über Remote-Aufrufe forciert wird).

Zusätzlich zur breiten Produktunterstützung ist in NCP ein so genannter Custom Patch Editor enthalten, mit dem sich individuelle Patches konfigurieren lassen. Das erfordert allerdings umfassende Kenntnisse in der XML-Programmierung, um die notwendigen Prüfungen umzusetzen. Auf diesem Wege lassen sich aber auch beliebige Produkte mit aufnehmen, wenn deren Hersteller von sich aus passende XML-Dateien liefern. Neben seiner Aufgabe als Patchtool kann NCP in gewissen Grenzen auch zur Softwareverteilung für die unterstützten Produkte genutzt werden, also unter anderem für Adobe Reader, Mozilla Firefox, Flash, Quicktime und Shockwave Player sowie alle .NET-Framework-Versionen. Vorsicht ist dahingehend geboten, weil die notwendige Einstellung unscheinbar und ein wenig versteckt ist, aber immense Auswirkungen hat, wenn ein Scanlauf mit einer anschließenden automatischen Patchverteilung gekoppelt ist. Dann werden womöglich auf Hunderten von Clients alle genannten Produkte (und noch einige mehr) nicht nur gepatcht, sondern gegebenenfalls auch erstmals installiert.

Mehr Features per Agent

Patches und Asset Management arbeiten agentenlos und können somit auf den Clients angewendet werden, ohne dass dort vorher etwas installiert werden muss. Darüber hinaus kommt mit NCP

ein Agent mit, der die zusätzlichen Features von NCP in Form von Viren- und Spywareabwehr aktiviert, der auf Wunsch aber auch das Patchen steuert. Um den Agenten zu installieren, sind einige Voraussetzungen zu beachten, wie eine zusätzliche Freischaltung in der Firewall der Clients (TCP-Ports 139 und 445), und dass der Remoteregistrierungsdienst sowie der Serverdienst laufen müssen.

Zum Betrieb der Agenten sind im Vorfeld Agenten-Policies, also wieder entsprechende Profile zu bauen, wobei darin für das Scannen und die Patchverteilung einfach bereits vorhandene Templates eingetragen werden. Der Agent durchsucht das System per Scheduler in frei wählbaren Abständen auf Bedrohungen durch Viren, Spy- und Malware. Der Administrator hat zudem die Möglichkeit, über entsprechende Ausnahmelisten bestimmte ausführbare Programme zu erlauben, zu sperren oder aber dem Anwender den Aufruf nochmals bestätigen zu lassen. Neben der Virensuche in Intervallen kann der Administrator eine Prüfung bei Dateizugriff aktivieren und vorgeben, wie das System auf bestimmte Aktionen reagieren soll (Änderung der Explorer-Sicherheitseinstellungen oder der System Policies, Aufruf von Programmen und so weiter). Bei der Abwehr von Viren und schädlichem Code arbeitet Shavlik mit Sunbelt zusammen und hat die schnelle sowie schlanke Vire-Engine integriert.

Im Test hinterließ der Agent allerdings einen etwas durchwachsenen Eindruck. Der Ansatz, verschiedene Funktionen auf diese Weise in einem Werkzeug zu

Produkt

Programm für das Patchmanagement im Windows-Umfeld.

Hersteller

Shavlik
www.shavlik.com, www.prosoft.de (Distributor)

Preis

Shavlik unterscheidet zwischen Lizenzen für Workstations und Server, 100 WS-Lizenzen kosten 4.920 Euro, 10 Server-Lizenzen 984 Euro mit einer Konsole, eine weitere Konsole kostet 1.836 Euro, für andere Mengen gibt es Staffelpreise.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Installation/Bedienung	8
Patchfunktionalität	9
Antivirus/Antispy-Funktion	6
Asset Management	4
Dokumentation	7

Dieses Produkt eignet sich

optimal für mittlere und größere Umgebungen im Windows-Umfeld, die auch den vollen Leistungsumfang nutzen wollen. Hier kann das Programm seine Stärken voll zur Geltung bringen.

bedingt in kleineren Umgebungen, wenn nur wenige Systeme zu aktualisieren sind und sich der Betriebsaufwand für ein derart mächtiges Werkzeug nicht lohnt. Aus finanzieller Sicht erscheint uns das Werkzeug auch dann nur bedingt geeignet, wenn es nur zum Patchen genutzt werden soll.

nicht, wenn Windows-basierende Systeme eine untergeordnete Rolle spielen, da die gesamte Verwendung auf diese Betriebssystemfamilie aufsetzt.

Shavlik NetChk Protect 7.1

vereinen, ist auf jeden Fall sehr interessant. Wir vermissen allerdings rund um Antivirus und Antispy entsprechende



Informationen für den Administrator. Es ist von der zentralen Konsole aus nicht auf einen Blick erkennbar, welche Signaturversionen im Einsatz sind und ob alle Clients auch mit den aktuellsten Signaturen arbeiten. Der Administrator kann zwar einen Report erstellen, bekommt dann aber jede Maschine extra aufgeführt. Insgesamt vermissen wir hier bessere Möglichkeiten zur Auswertung, die gezielt auf einen Handlungsbedarf hinweisen. Besser ist die Information auf Clientseite, hier liefert der Agent genaue Informationen zu den Versionen und zum letzten Suchlauf.

Für ein erstes Reporting zeigt NCP bereits auf der Startseite eine Handvoll von Balkengrafiken zur Darstellung des allgemeinen Patchstandes an. Allerdings machen diese TOP-10-Anzeigen auf uns eher einen plakativen Eindruck, als dass sie wirklich weiterhelfen. Auch kann man nicht einfach auf solch eine Darstellung klicken, um dann weitere Detailinformationen zu erhalten. Auf

jeden Fall hilfreicher ist die eigentliche Reportfunktion, die eine geschickte Auswahl und Filterung mit wenigen Mausklicks erlaubt. Mehr als 20 Reports sind dabei fest integriert, die Darstellung ist für eine Druckausgabe vorbereitet. Vorteilhaft ist, dass sich auf Wunsch ein automatisches Mailing per SMTP einrichten lässt.

Fazit

NetChk Protect überzeugt nach wie vor mit einem absolut leistungsfähigen Patchmanagement im Windows-Umfeld für das Betriebssystem selbst, für weitere Microsoft-Produkte sowie diverse weit verbreitete Programme. Die vielfältigen Funktionen erfordern allerdings eine gewisse Einarbeitung, und eine Einführung in einem Unternehmen setzt eine gezielte Planung voraus. Dabei ist NetChk Protect durch die Möglichkeit, sowohl mit mehreren Distributionsservern als auch mehreren Konsolen zu arbeiten, auch für sehr große Umgebungen geeignet.

Die Module Antivirus, Antispy sowie das ganz neue Asset Management zeigen durchaus den richtigen Weg auf, um die Anzahl der Werkzeuge, die für ein effizientes Clientmanagement erforderlich sind, sinnvoll zu reduzieren. Sie erscheinen uns aber insgesamt noch optimierungsbedürftig. Bei den Funktionen Antivirus und Antispy vermissen wir eine zentrale Statusübersicht, beim Asset Management die Möglichkeiten zur weiteren Nutzung und Verarbeitung der ermittelten Daten. Eine ganz andere Problematik bei derartig integrierten Lösungen ist natürlich die Tatsache, dass ein Unternehmen beispielsweise gerne mit NCP patchen möchte, aber einen anderen Virens Scanner bevorzugt und vielleicht schon ein Werkzeug zur Softwareverteilung und Inventarisierung besitzt. Mit einem integrierten Werkzeug wird es sicher nicht einfacher, alle Kunden zufrieden zu stellen, wobei diese stets den gesamten Leistungsumfang von NCP bezahlen müssen. (jp)

