7 | 20 Sonderdruck für NinjaRMM

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

NinjaRMM

www.it-administrator.de

Quelle: kenishirotie – 123RF

NinjaRMM

Flottenmanager

von Thomas Bär und Frank-Michael Schlede

Ganz gleich ob Managed Service Provider oder eigene IT-Abteilung: Die IT-Mitarbeiter müssen die Geräte und das Netzwerk der jeweiligen Organisation gut im Griff behalten. Hier will dem Admin die Software NinjaRMM unterstützend zur Seite stehen. Sie nimmt für sich in Anspruch, die Verwaltung und das Management der Endpunkte besonders nutzerfreundlich und intuitiv zu lösen. Tatsächlich lässt das Produkt kaum Wünsche offen.

In der an Abkürzungen sicher nicht armen IT-Welt dürfte RMM (Remote Monitoring Management) vor allen Dingen in den Unternehmen gut bekannt sein, die sich als Managed Service Provider (MSP) um die IT-Belange anderer Firmen kümmern. Bei RMM handelt es sich in der Regel um eine Softwareplattform, die MSPs dabei helfen soll, die Endpunktgeräte, Netzwerke und ganz allgemein Computer ihrer Kunden remote und proaktiv zu überwachen und zu betreuen.

Zugang nur mit Zwei-Faktor-Authentifizierung

Das Unternehmen NinjaRMM wurde 2013 im Silicon Valley gegründet, wo sich heute noch der Hauptsitz befindet. In Deutschland besitzt die Firma eine Niederlassung in Berlin. Wir bekamen vom Hersteller einen Testzugang, der es uns ermöglichte, die Features und Möglichkeiten der Software zu betrachten.

Wer mit NinjaRMM starten will, braucht zunächst nur einen Zugang zur SaaS-Plattform. Dieser setzt standardmäßig voraus, dass der Nutzer eine Zwei-Faktor-Authentifizierung, beispielsweise via SMS auf ein Smartphone, einrichtet. Das funktionierte sofort und ohne Probleme, nachdem wir auf der Webseite des Unternehmens ein eigenes Konto eingerichtet hatten.

Hilfreiche Onlinedokumentation

Nach der Anmeldung findet der Nutzer im Browser ein übersichtliches Dashboard. Was hier gleich zu Beginn ganz besonders gefällt: Der Anwender bekommt zunächst eine Seite mit ersten Schritten angezeigt, die ihn sehr einfach durch die Einrichtung der Software führen. Wer sich bereits genug eingearbeitet hat, kann diese Seite später auf Wunsch ausblenden. Wir haben sie allerdings während der gesamten Testphase als sehr hilfreich empfunden.

Zudem kann der Administrator jederzeit direkt aus der Oberfläche heraus auf die Onlinedokumentation zugreifen, die zum Großteil in deutscher Sprache bereitsteht. Etwas unpraktisch fanden wir dabei, dass es nach jedem neuen Anmelden nötig war, beim Zugriff auf die Dokumentation diese immer wieder händisch auf die deutsche Sprache einstellen zu müssen, wo sich doch die gesamte Oberfläche bereits in Deutsch präsentierte. Das ist wohl

NinjaRMM

Produkt
SaaS-basierte Fernwartungs- und Verwaltungsplattform.

Hersteller
NinjaRMM
www.ninjarmm.com/de/

Preis
NinjaRMM ist pro Gerät und Monat ab 4,50 Euro erhältlich.

Systemvoraussetzungen
Zum Aufruf des Dashboards kann jeder gängige Browser zum Einsatz kommen. Auf Seite der Agenten unterstützt die Software Windows-Desktopsysteme ab Windows Vista, Serversysteme ab Windows Server 2008 und Apple macOS ab macOS 10.10 (Yosemite). Wer Netzwerkgeräte mittels NMS (Network Management System/ Network Management Station) verwalten möchte, sollte die Software auf Windows Server installieren. Zu Testzwecken ist eine Installation auf Windows 7/8/10 möglich, die aber laut Hersteller nicht für den Produktivbetrieb geeignet ist.

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

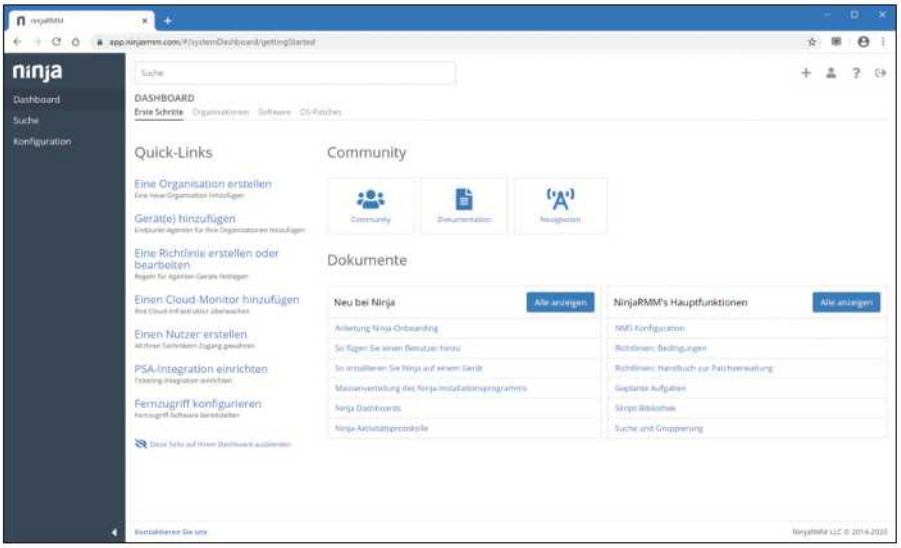

Bild 1: Beim ersten Anmelden an NinjaRMM präsentiert das Dashboard übersichtliche und gut strukturierte Hilfen in geordneter Reihenfolge.

darauf zurückzuführen, dass die Dokumentation auf einer "Dojo" genannten Webseite zu finden ist. Diese stellt zwar auch deutschsprachige Beiträge bereit, doch gelang es uns nicht, unser Profil dort standardmäßig auf "Deutsch" festzulegen.

Übersichtliches Dashboard

Auf der linken Seite des Browserfensters findet der Administrator ein Menü mit allen Einstellungen und Untermenüs. Im Bereich Konfiguration kann er dann im Untermenü "Allgemein" die Einstellung für die Zeitzone, den Namen der eigenen Organisation und die Settings für Benachrichtigungen festlegen, die er selbst erhalten möchte. Bei diesen Einstellungen fanden wir eine kleine Kuriosität: Bei der Wahl der Zeitzone fehlt eine deutsche Stadt (normalerweise steht an dieser Stelle immer Berlin). Das ist sicher kein Problem, befinden wir uns doch in der gleichen Zeitzone wie Brüssel oder Amsterdam – aber bei der Länge der Liste der angebotenen Orte fällt es dennoch auf.

Wer danach mit dem Onboarding seiner Geräte beginnen will, sollte zunächst eine neue "Organisation" erstellen. Damit sind hier die einzelnen Kunden gemeint, deren Geräte und Netzwerke mithilfe von NinjaRMM betreut werden sollen. Standardmäßig findet der Nutzer in der Software zunächst nur unter "Internal Infrastructure" das eigene Netzwerk. Wer nicht als MSP tätig ist, kann auf diese Weise Teile des eigenen Firmennetzwerkes organisieren.

Nach dem Wechsel zu "Organisation" im Konfigurationsmenü kommt der Administrator mit einem Klick zu "Neue Organisation erstellen" in einem weiteren Menü, in dem er diese Organisationseinheit anlegen kann. Wie in allen anderen Menübereichen der Software kann er dazu aber auch das große Pluszeichen in der rechten oberen Ecke des Browserfensters auswählen. Daraufhin öffnet sich der Organisationseditor, in dem der Nutzer dann neben der allgemeinen Beschreibung der Organisation unter anderem das Zeitfenster konfiguriert, in dem ihm Benachrichtigungen zu dieser Organisation geschickt werden. Hier kann er somit einen Abgleich mit den SLA-Vereinbarungen anstellen, die mit dem Kunden getroffen wurden.

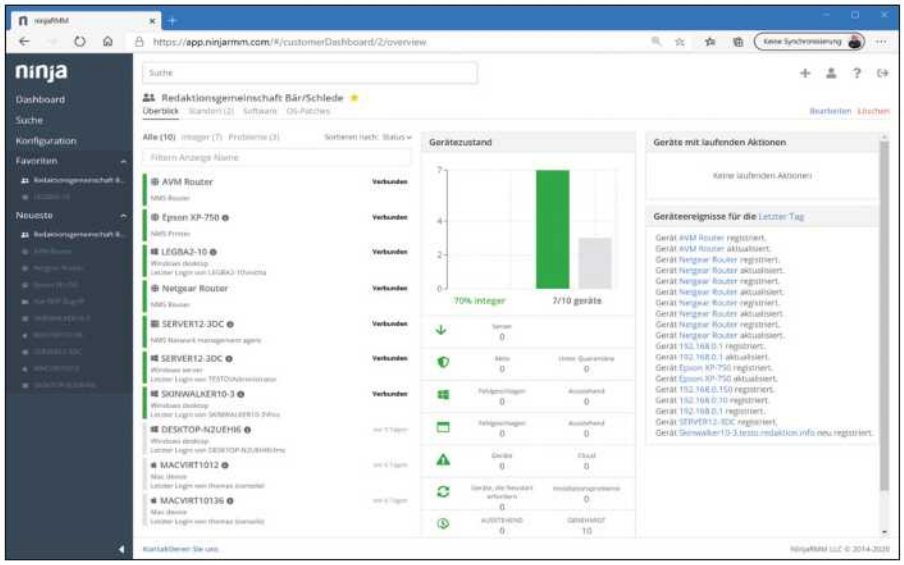

Bild 2: Die von uns schnell eingerichteten Systeme waren sofort und leicht einsehbar, auch wenn sie virtuell betrieben wurden.

Nützliche Richtlinien und Gerätegruppen

Im Bereich "Sicherheit" steht die Konfiguration der Genehmigungseinstellungen für Geräte bereit: An dieser Stelle erlaubt der Administrator beispielsweise eine automatische Genehmigung für Geräte in dieser Organisation, erstellt aber auch die generelle Verweigerung für neue Geräte sowie eine grundsätzlich manuelle Konfiguration. Diese Genehmigungen lassen sich zudem im Dashboard des jeweiligen Unternehmens ändern. Weiterhin können die IT-Mitarbeiter in diesem Editor unter anderem festlegen, welche Standard-Anmeldeinformationen Verwendung finden und welche Richtlinien in der Organisation für welche Geräte zum Einsatz kommen sollen.

Ebenfalls im Konfigurationsmenü finden sich die Richtlinien. Eine solche Richtlinie besteht laut Anbieter aus einer Reihe von Bedingungen, Aktionen und verschiedenen Einstellungen wie Windows- und Software-Patchmanagement, Remotezugriff und Virenschutz, die gemeinsam auf eine Gruppe von Geräten anwendbar sind, die Mitglieder dieser Richtlinie sind. Der Nutzer bekommt mit der Bereitstellung der Software bereits eine Liste von sogenannten Standardrichtlinien mitgeliefert. Sie bieten Standardeinstellungen zur Überwachung der Geräte. Grundsätzlich unterscheidet die Software dabei Richtlinien für die Agenten, für die virtualisierten Systeme (ausschließlich für VMware) und für

NMS-Richtlinien (Network Management System) für Netzwerkgeräte.

Granulierbare Berechtigungen

Natürlich lassen sich im Konfigurationsmenü auch neue NinjaRMM-Nutzer für den Zugriff anlegen. Dabei können Administratoren beispielsweise entscheiden, ob neue Nutzer standardmäßig eine Multifaktor-Authentifizierung (MFA) bei der Anmeldung nutzen müssen. Das funktionierte bei unserer Testinstallation problemlos und der neue Nutzer wurde aus dem System heraus mittels E-Mail darüber informiert, dass er nun auf das System zugreifen konnte. Dabei gilt es zu beachten, dass ein solcher Nutzer zunächst konfiguriert und gespeichert sein muss, bevor sich die MFA erstmalig aktivieren lässt.

Beim Anlegen eines neuen Nutzers (oder später via "Bearbeiten") wählen Systemverwalter zwischen drei MFA-Methoden: Neben der Verifizierung mittels SMS kann wahlweise auch eine sogenannte Authenticator-App wie beispielsweise Google Authenticator oder ein U2F-USB-Schlüssel (Universal Second Factor) zum Einsatz kommen. Bei den Berechtigungen für den Nutzer ist die Auswahl zwischen den Rechten als Systemadministrator oder "Benutzerdefiniert" möglich. Wählt der Administrator "Benutzerdefiniert", stehen ihm sehr fein granulierte Einstellungen für die Berechtigungen zur Verfügung. Auf diese Weise kann er dann zum Beispiel Nutzer konfigurieren, die als Systembetreuer für Teilbereiche tätig sind.

Agenten für Windows, macOS und Netzwerk

Ist eine Organisation eingerichtet und befinden sich Richtlinien im System, kommt der Administrator über einen Klick auf das Plus-Symbol in der Weboberfläche zum Eintrag "Gerät hinzufügen". Hier hat er die Wahl zwischen Windows, macOS und NMS (Netzwerkgeräte). Nach der Auswahl von Windows oder macOS muss er dann noch die Organisation und den Standort (hier ist "Main Office" standardmäßig vorgewählt) bestimmen und kann anschließend das Feld "Installer generieren" auslösen. Während bei Windows automatisch eine MSI-Datei erstellt wird, hat der Nutzer bei einem Apple-System die Wahl zwischen einem Installer im PGK- und einem im DMG-Format.

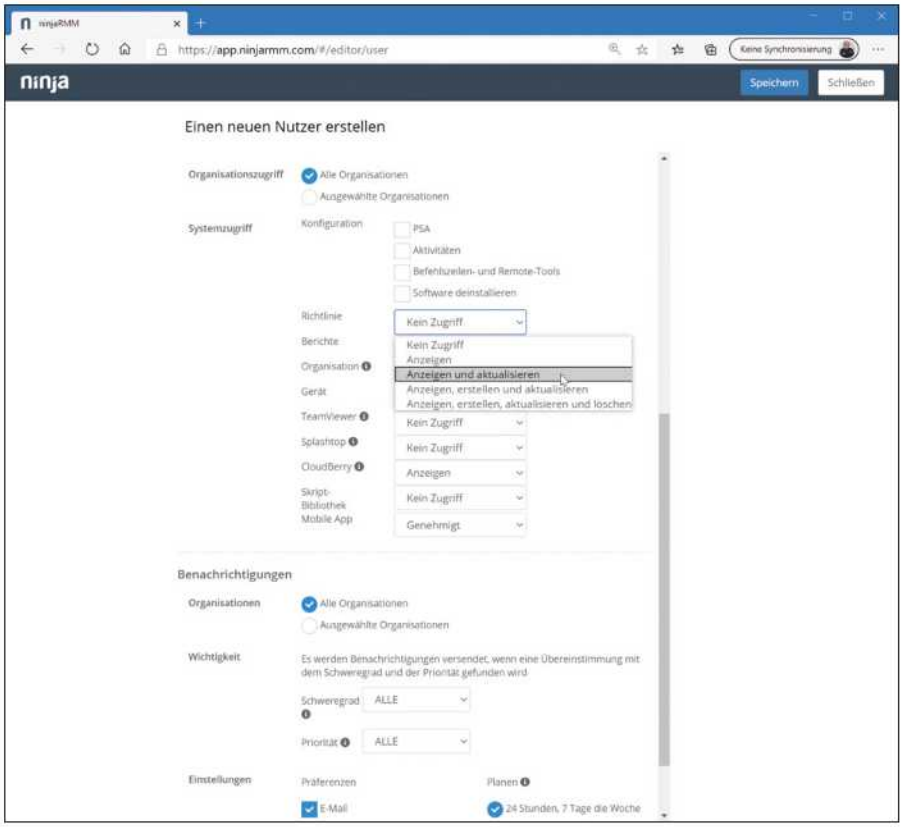

Bild 3: Sehr fein granulierte Einstellungen für die Berechtigungen lassen sich für einzelne Teilbereiche bestimmen.

Das Generieren dauert einen kleinen Augenblick und danach lässt sich das Installer-Paket herunterladen. Die MSI-Datei ist dabei mit 28 MByte relativ klein. Im Dateinamen finden sich sowohl der Name der Organisation als auch der des Standortes des jeweiligen Geräts wieder. Natürlich kann das MSI-Programm auch mittels der üblichen Verteilmechanismen auf die Endgeräte gelangen. Der Hersteller beschreibt in der Dokumentation diesen Weg mithilfe der Software PDQ Deploy oder mittels des Sysinternal-Tools PsExec.

Wir haben in unserem Testnetz sowohl auf verschiedenen physisch vorhandenen Windows-10-Systemen als auch auf einem unter VMware-Workstation virtualisierten Windows-2012-Server und unter Parallels virtualisierten Apple-Systemen (macOS 10.13 und macOS 10.12) installiert. Die Installation verlief bei allen Systemen einfach und schnell und in den Standardeinstellungen "verschwindet" der Agent vollständig von der Oberfläche des Systems, ist also nur noch als Prozess zu finden. Administratoren können die Agenten aber auch so konfigurieren, dass sie, wie bei vielen derartigen Lösungen üblich, auf dem Windows-System im Systray erscheinen. Das Erscheinungsbild dieses Icons können die Systemverwalter dabei weitgehend der eigenen Firma anpassen und den Nutzern auf diese Weise zum Beispiel eine "Ein-Klick"-Kontaktadresse zur Verfügung stellen.

Skriptübermittlung gut gelöst

Die wichtigen Systemdaten der einzelnen Systeme haben die Agenten zuverlässig an den NinjaRMM-Server übermittelt. Sie ließen sich dann im Dashboard direkt unter "Details" auslesen. Hier findet ein Systembetreuer bei Windows-Systemen dann unter anderem die Infos zu den Datenträgern, zum Speicher sowie zu auf dem System offenen Ports und kann auch Ereignis- und Nutzerprotokolle einsehen. Ein Zugriff auf die mitgelieferte Skript-Bibliothek ist ebenfalls direkt möglich: Der Administrator kann dann die vorhandenen Skripte direkt auf dem System ablaufen lassen.

Auch während des Onboardings lassen sich den Systemen Skripte mitgeben. Wir

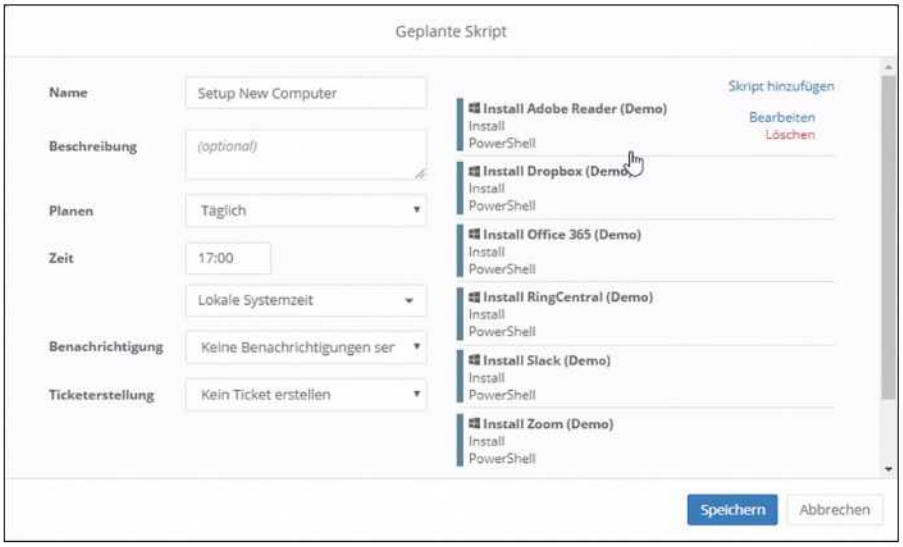

Bild 4: Mittels Skripten ist konfigurierbar, welche Anwendungen auf neuen Windows-Systemen standardmäßig installiert werden sollen.

haben das bei den Apple-Systemen mit den vom Hersteller mitgelieferten Skripten für "Neustart" und "Updates ausschalten" durchgespielt, was einwandfrei funktionierte. Die Systemverwalter können zudem direkt in der Ninja-Oberfläche eigene Skripte beispielsweise mittels PowerShell einpflegen und nutzen. Uns hat dabei besonders gut gefallen, dass ein Administrator direkt aus der GUI via Terminal oder der PowerShell unter Windows auf das System zugreifen kann, wenn er die richtigen Berechtigungen besitzt.

Eine Software-Inventurliste liefert die Lösung ebenfalls. Während der gesamten Testphase wurden alle noch so kleinen Änderungen, wie etwa ein Update des Firefox-Browsers auf einer Arbeitsstation, protokolliert und gemeldet. Auch ein größerer Eingriff wie die nachträgliche Änderung der RAM-Größe eines unserer Apple-Systeme wurde bemerkt und protokolliert. Bei der Auflistung der installierten Software würden wir uns nur noch eine zusätzliche Filtermöglichkeit wünschen, die es erlaubt, eine Suche in der Form "alle Software, die nicht von Apple oder Microsoft ist" zu starten.

Eigener Server fürs SNMP-Monitoring

Die dritte Option bei der Installation von Agenten betrifft die Überwachung von Netzwerkgeräten. Mit diesem Agenten können die Systembetreuer dann beispielsweise Router, Drucker und Switches überwachen. Wählen Sie diese Option aus, bekommen Sie eine ausführbare Windows-Datei in der Größe von etwa 200 MByte bereitgestellt. Dieser Agent ist von der Installation eines Windows-Agenten getrennt, lässt sich aber problemlos auf einem Windows-Server installieren, auf dem bereits ein Windows-Agent läuft. Das hat in unserer Testumgebung auf einem Windows-2012-R2-System problemlos funktioniert.

Für jede Organisation beziehungsweise im Falle eines MSPs für jeden Kunden, bei dem SNMP-Geräte überwacht werden sollen, ist ein solcher Agent zu installieren. Zu Testzwecken kann das zwar auf einem Windows-7/8/10-System erfolgen, der Hersteller rät aus Performancegründen aber davon ab. Als ideale Plattform schlägt NinjaRMM einen Windows-Server ab der Version 2008 vor, wobei die Software sowohl die 32- als auch die 64-Bit-Version des Server-Betriebssystems unterstützt. Während die anderen Agenten keine weiteren Softwarevoraussetzungen erwarten, muss für diesen NMS-Agenten das .NET-Framework ab der Version 4.7 installiert sein.

Nach der Installation und einem Neustart des Servers meldet sich der Administrator dort mit seinen NinjaRMM-Zugangsdaten an. Dann wählt er die Organisation aus, der er die SNMP-Geräte zuweisen möchte. Mittels der dann folgenden manuellen Netzwerkerkennung im Programm kann der Admin daran anschließend das Netzwerk scannen. Die Software überprüft alle Geräte im angegebenen IP-Subnetz oder der IP-Gruppe. Sie unterstützt SNMP v1, v2c und v3. NinjaRMM weist den gefundenen Geräten dabei automatisch die richtigen Rollen zu, wenn sich der Gerätetyp ermitteln ließ. Der NMS-Agent sendet SNMP-Traps an die entsprechenden Geräte und kann SNMP-Antworten und Traps sowie Syslog- und NetFlow-Informationen von den Geräten sammeln und diese dann an den Ninja-Server weiterreichen, sodass der IT-Verantwortliche sie in seinem Dashboard findet.

Umfangreiches Berichtswesen

Nicht unerwähnt darf die sehr gute Unterstützung für Berichte bleiben – ein Bereich, der ganz besonders im Umfeld der MSPs von hoher Bedeutung ist. Im Menü "Konfiguration" findet der Nutzer den entsprechenden Punkt. Hier kann er dann einen neuen Report anstoßen oder auf bereits vorhandene Berichte zugreifen. Wer einen neuen erstellen will, hat die Auswahl zwischen vordefinierten Berichten mit den Bezeichnungen "Regulär", "Executive Summary", "Anlagenbericht", "Patch-Compliance" und "Benutzerdefiniert". Auch hier war als Standardeinstellung leider immer wieder "English (en-us)" für die Spracheinstellung vorgewählt. Das ist zwar eine Kleinigkeit, aber wenn schon die gesamte Oberfläche auf eine bestimmte Sprache eingestellt ist, dann sollte sich das auch hier widerspiegeln.

Nach der Auswahl der Organisation, über die es einen Bericht zu erstellen gilt, kann der Administrator dann noch die E-Mail-Adresse der Adressaten und den zeitlichen Umfang des Reports wählen. Er bestimmt die Frequenz und die Uhrzeit des Versands. Wählt der Nutzer zum Beispiel die Berichtsform "Regulär", findet er bei den Inhalten unter der Überschrift "Abschnitte" eine große Anzahl von Daten, die in seinem Bericht Erwähnung finden. Diese kann er aber auch einzeln abwählen. Die meisten Möglichkeiten bietet dabei der Bericht mit dem Label "Benutzerdefiniert". Hier kann der Administrator aus einer sehr großen Anzahl von Abschnitten auswählen, die Teil seines Berichts werden sollen. Das geht

So urteilt IT-Administrator

Dashboard und Konfiguration	8
Agenteninstallation & -betrieb	9
Richtlinienmanagement	9
Scripting-Unterstützung	8
Berichte erstellen	8

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für MSPs, die Überwachung und Betreuung von IT-Netzen als Dienstleistung anbieten. Aber auch für größere IT-Organisationen mit mehreren Standorten, die damit die Geräte im eigenen Netzwerk überwachen und betreuen wollen.

bedingt für kleinere Unternehmen, in deren Netz sich nur wenige Geräte befinden und das sich auf einen oder zwei Standorte beschränkt.

nicht für Solo-Selbstständige und kleine Bürogemeinschaften.

hin bis zur Auflistung der Produktschlüssel der Windows-Systeme.

Erst mit der aktuellen Version 4.5 der Software, die wir uns angeschaut haben, ist noch der Abschnitt "Antivirenbericht" hinzugekommen. Dieser sammelt aber im Moment nur die Daten aus dem Microsoft Security Center, wenn dieses in den Systemen auch aktiviert ist – was gerade auf den Windows-Servern nicht immer der Fall ist. Ninja bietet dort allerdings zudem einen integrierten AV-Schutz an (Webroot oder Bitdefender), dessen Daten auch dann gemeldet werden, wenn er auf einem Windows-Server ohne aktiviertes Security Center zum Einsatz kommt.

Fazit

Die Software von NinjaRMM konnte im Testeinsatz überzeugen. Dabei hat uns besonders gut gefallen, wie das RMM-Werkzeug neue Nutzer an Einsatz und Betrieb heranführt. Insgesamt sind Nutzerführung und Oberfläche sehr gut strukturiert, sodass es einem erfahrenen Administrator kaum Probleme bereiten dürfte, die Software für seine Kunden beziehungsweise Mitarbeiter in der Firma einzusetzen.

Auch wenn die Hauptzielgruppe des Anbieters nach wie vor bei den MSPs zu finden sein dürfte, denken wir, dass ebenso Administratoren in mittelgroßen und großen Firmennetzwerken diese Art des Remote-Managements gut einsetzen können. Gerade in der aktuellen Situation, in der die Mitarbeiter immer häufiger aus entfernten Standorten und Home Offices auf das Firmennetzwerk und die Daten darin zugreifen müssen, kann eine solche Software die Arbeit der IT-Mannschaft deutlich erleichtern.

In diesem Zusammenhang möchten wir noch einmal die Agentensoftware loben: Wir haben schon diverse Produkte getestet, die ihre Agenten auf die Endpunkte verteilten. Dabei war aber bis jetzt keine, deren Software auf den Windows- und macOS-Systemen so klein ist und unauffällig wie zuverlässig gearbeitet hat. Wer auf sehr strenge Sicherheitsvorschriften für seine IT und deren Daten Rücksicht nehmen muss, sollte beachten, dass die Firma ihre Server auf AWS hostet. *(ln)*