Probleme im Netzwerk erkennen und beseitigen

Die IT-Verantwortlichen in Unternehmen haben es in ihrem Arbeitsalltag mit mannigfachen Herausforderungen zu tun. Eine Netzwerk-Monitoring-Software kann sie dabei unterstützen: Sie überwacht die gesamte IT-Infrastruktur und alarmiert die IT-Abteilung, sobald etwas „Ungewöhnliches" passiert.

Störungen im Netzwerk treten meist unangekündigt auf. Beruhigt kann der Admin indes arbeiten, wenn ihm eine Überwachungssoftware als Freund zur Seite steht. Im Folgenden zeigen typische Fälle aus dem Alltag, wie ein Administrator Störfälle durch den Einsatz einer Monitoring-Software einfacher in den Griff bekommt.

Die Bedürfnisse des Netzwerks auf einen Blick

Potenzielle Hardwareprobleme früh erkennen

Ein Administrator hat unter anderem die Aufgabe, die Hardwarekomponenten der Infrastruktur täglich zu prüfen. Die Leistung von CPU , Speichergeräten , Servern und Co. sollte gleichbleibend hoch sein.

Eine Netzwerk-Monitoring-Lösung hilft ihm, den Status dieser Komponenten zu überwachen. Sie liefert detaillierte Daten und Langzeitberichte zur gesamten Hardware. Durch Analyse dieser Informationen kann der IT-Verantwortliche Trends erkennen und den Optimierungsbedarf bestimmen. Die Software alarmiert ihn sofort, wenn eingerichtete Schwellenwerte überschritten werden oder falls Serverausfälle auftreten. Auf diese Weise ist es für den Administrator möglich, vorausschauend zu agieren statt nur zu reagieren.

Fehlerhafte Windows-Services und Server-Neustarts

Innerhalb der IT-Infrastruktur eines Unternehmens sind viele Server und Services aktiv. Kommt es zu Fehlern, kann es zur Problembehebung notwendig werden, den Server neu zu starten. Wenn Admins die Windows-Services via Netzwerk-Monitoring überprüfen lassen, erhalten sie bei Ausfällen eine Benachrichtigung etwa per SMS oder E-Mail, aber ein Neustart muss manuell ausgeführt werden.

Effizienter wäre es, wenn der Neustart des Servers automatisch ausgelöst wird, ohne Zutun des Admins. Mit dem Benachrichtigungssystem der Monitoring-Software ist dies möglich. Dazu erstellt der Administrator ein Skript, das einzelne Ser-

vices oder den kompletten Server rebooten kann. Wenn ein Service oder Server für eine bestimmte Zeitspanne „down" ist, führt die Monitoring-Software dieses Skript über eine spezielle Art von Benachrichtigung aus, und der Neustart erfolgt automatisch. Ein standardmäßig verfügbarer Sensor sollte Windows-Services mit einer entsprechenden Option bei einem Ausfall auch automatisch neu starten.

Geplante Ausfallzeiten stressfrei überstehen

Ausfälle von Servern geschehen nicht immer ungeplant. Ab und zu ist es erforderlich, Netzwerkgeräte planmäßig außer Betrieb zu setzen – zum Beispiel für Wartungsarbeiten oder einfach, um Systeme am Wochenende oder über Nacht herunterzufahren. Damit die Überwachungslösung in diesen Zeiträumen der geplanten Downtimes nicht unnötig falsche Alarme auslöst, kann der Administrator das Monitoring zeitweise pausieren lassen. Dies sollte über zuvor festgelegte Zeitpläne auch für einzelne Netzwerkkomponenten automatisch erfolgen.

Qualität und Sicherheit im Netzwerk gewährleisten

Sicherheitsprobleme im Netzwerk erkennen

Vor Malware-Gefahren schützen sich die meisten Unternehmen mittels Security-Lösungen wie etwa Antiviren-Scanner oder Firewalls. Dadurch fühlen sie sich ausreichend abgesichert. Doch auch die Sicherheitssoftware ist nicht vor Ausfällen gefeit. Daher überprüfen Administratoren stetig, ob Antivirensoftware und Firewalls auf allen Computern laufen und up-to-date sind. Des Weiteren sollte die aktuelle Windows-Version auf dem neuesten Stand sein, und Security-Updates sollten lückenlos durchgeführt werden. Trotz aller Sicherheitsmaßnahmen kann das Unternehmensnetzwerk Cyber-Attacken zum Opfer fallen. Ungewöhnliche CPU-Last beziehungsweise Traffic-Spitzen können Anzeichen dafür sein.

Eine gute Netzwerkmanagementsoftware erkennt dies und schaltet die dazugehörigen Sensoren in einen Status, der „ungewöhnliche Werte" anzeigt. Zusätzlich überwacht die Monitoring-Software den allgemeinen Sicherheitsstatus, zum Beispiel die Antivirensoftware eines Windows-Computers mit WMI-Security-Center-Sensoren oder Windows-Server-Updates mit WSUS -Statistics-Sensoren. Eine andere hilfreiche Funktion für das Security-Monitoring ist die „Similar-Sensors-Analyse". Sie kann dabei helfen, verdächtige Abhängigkeiten zwischen Sensoren zu erkennen. Dank dieser vielfältigen Überwachungs- und Analysemöglichkeiten steigert die Monitoring-Lösung die Sicherheit im Netzwerk.

Physische Sicherheit im Data Center

Neben der Netzwerksicherheit hat auch die physische Sicherheit Priorität : Hohe Temperaturen, Feuchtigkeit, Wasserlecks, Feuer oder Rauch könnten die Ausrüstung eines Serverraums oder eines Rechenzentrums beschädigen. Um sicherzustellen, dass alle Geräte außer Gefahr sind, ist es ratsam, auch Umgebungsparameter zu monitoren. Mittels Hardwaresensoren für Temperatur oder Feuchtigkeit identifiziert die Software, wenn ungewöhnlich hohe Werte auftreten. Wenn zum Beispiel eine APC-Sensor-Box Temperaturen über 27 Grad misst, wird der IT-Verantwortliche alarmiert. Die Monitoring-Software kann auch die Funktion aller installierten Überwachungskameras prüfen, oder sie checkt, ob alle Türen und Fenster verriegelt sind, wenn die Mitarbeiter am Abend das Gebäude verlassen.

Webseiten hochverfügbar halten

Die Webseite ist für Firmen das Aushängeschild schlechthin. Internetauftritt inklusive gegebenenfalls vorhandenem Webshop spiegeln das Unternehmen und seine Leistungen digital wieder. Demnach ist deren Verfügbarkeit von enormer Bedeutung. Ist die Webseite nicht rund um die Uhr erreichbar, kommt es zu langen Ladezeiten oder scheitern beispielsweise die Kaufprozesse im Webshop an technischen Fehlern, könnten Anbieter dadurch Kundschaft verlieren.

Um mögliche Verluste zu vermeiden, sollte die Netzwerküberwachungslösung sofort warnen, wenn die Webseite ungewöhnliches Verhalten aufweist, also zum Beispiel sehr langsam ist. Das Monitoring nutzt unter anderem HTTP-Full-Web-Page-Sensoren, um die Ladezeiten der Seite zu überprüfen. Der http-Transaction-Sensor misst darüber hinaus den erfolgreichen Abschluss von Transaktionen auf einer interaktiven Webseite. Zudem steht dem IT-Personal etwa ein http-Apache-ModStatus-Totals-Sensor zur Verfügung, der Webseiten-Zugriffe und übertragene Daten prüft, um Lastspitzen zu bestimmten Zeiten zu identifizieren. So kann der Administrator auch erkennen, wenn mehr Bandbreite zur Verfügung gestellt werden muss.

Quality-of-Service überprüfen

Für die Business-Kommunikation sind die Tonqualität von Voice-over-IP (VoIP)-Verbindungen sowie das Video-Streaming immens wichtig. Hakt es bei solchen Verbindungen, müssen Administratoren die relevanten Parameter der Netzwerkverbindung (Jitter, Packet Loss oder Packet Delay) untersuchen. Welche Parameter könnten für das Problem verantwortlich sein? Sowohl VoIP als auch Video-Streams verlassen sich auf einen stetigen Strom von Datenpaketen. Die Quality-of-Service leidet zum Beispiel, wenn UDP (User Datagram Protocol)-Pakete nicht rechtzeitig empfangen werden oder verloren gehen.

Professionelle Netzwerk-Monitoring-Lösungen sollten einen vorkonfigurierten Quality-of-Service (QoS)-Sensor bieten, mit dem Administratoren die Qualität der Netzwerkverbindungen messen können. Durch die detaillierten Informationen können IT-Abteilungen den Optimierungsbedarf präzise bestimmen und entsprechende Probleme oder Engpässe rechtzeitig beheben.

Basissysteme im Blick behalten

Schlechte Datenbank-Performance

Im Arbeitsalltag greifen Mitarbeiter auf unzählige Daten aus dem Unternehmensnetzwerk zu. Weisen die internen Datenbanken eine schlechte Leistung auf, lähmt dies die Arbeitsprozesse in der gesamten Firma. Die alltägliche Aufgabe des Admins besteht also auch darin, die Leistungsindikatoren der Datenbanken zu überprüfen.

Schwankt die Leistung einer Datenbank, müssen IT-Verantwortliche die Gründe dafür finden. Diese Suche kann eine langwierige Aufgabe sein. Eine professionelle Monitoring-Software unterstützt das IT-Personal bei der Leistungssteigerung der Datenbank. Beispielsweise zeigen WMI-SQL-Server-Sensoren die Anzahl von Nutzerverbindungen an. Ist die Leistung zu bestimmten Zeiten schlecht, könnten zu viele Nutzer zeitgleich aktiv sein. Ist dies der Fall, wäre es Administratoren zum Beispiel möglich, den verfügbaren Speicher auf dem SQL-Server zu erhöhen und das Problem aus der Welt zu schaffen.

Unzuverlässiges Verhalten in virtuellen Umgebungen

In Zeiten hochflexibler IT-Infrastrukturen spielt die Virtualisierung eine große Rolle für den Administrator. Er sollte die virtuellen Systeme immer im Blick haben. Eine Netzwerk-Monitoring-Software bietet verschiedene Sensoren zur Überwachung virtualisierter Umgebungen an. Unter anderem kann das IT-Personal die CPU- und Speicherauslastung, die Netzwerkgeschwindigkeit sowie die Gesamt-Performance virtueller Maschinen überwachen.

Die meisten Netzwerk-Monitor-Tools unterstützen dazu etwa die Plattformen VMware vSphere , Microsoft HyperV , Citrix Xen und Virtuozzo . Auch den Status der Host-Server haben die Administratoren immer im Blick. So können Administratoren unmittelbar erkennen, ob das Problem in der virtuellen Maschine liegt oder von der Host-Hardware verursacht wird. Misst einer der Sensoren auffällige Werte, zeigt die Netzwerk-Monitoring-Lösung dies an und sendet eine Nachricht an den zuständigen IT-Verantwortlichen.

Backups überblicken

In der IT-Infrastruktur werden verschiedene Backups durchgeführt: Im Bereich der Virtualisierung, im Betriebssystem, bezüglich SQL und Exchange sowie online laufen täglich Datensicherungen ab. Hier hilft Administratoren eine Backup-Software. Diese Lösungen senden meist E-Mails, die den Status der nächtlich ablaufenden Datensicherungen bekannt geben. Aber für den Administrator ist es nicht einfach, den Überblick über all diese Backup-Prozesse zu behalten. Er müsste Unmengen von E-Mails analysieren, bis er endlich ein Backup-Problem identifizieren kann.

Allerdings können IT-Verantwortliche ihre Software so konfigurieren, dass sie alle Status-E-Mails an ein Postfach sendet, wo sie mit IMAP-Sensoren des Netzwerk-Monitorings automatisch analysiert werden. Auf diese Weise behält die Überwachungslösung den Überblick über alle Datensicherungen, meldet, wenn Backups nicht ordnungsgemäß durchgelaufen sind – und der Administrator ist entlastet.

Zeitaufwendige Wartung der Drucker

Wegen der vielen wichtigen Aufgaben des Arbeitsalltags möchte der IT-Administrator seine knappe Zeit nicht damit verbringen, jeden Tag den Status aller Drucker manuell zu checken. Es ist nervig, wenn man konzentriert bei der Arbeit ist und wegen Papiermangel oder Papierstau gerufen wird. Eine Monitoring-Lösung schafft hier unter anderem mit Windows-Print-Queue-Sensoren Abhilfe. Die Sensoren überwachen alle Aufträge auf einem Druckerserver. Wenn das Papier zur Neige geht, erhält der Administrator rechtzeitig eine Warnmeldung und kann zu passender Zeit reagieren, bevor Anfragen von Kollegen eintreffen. Zudem ist das IT-Personal in der Lage, die Überwachungssoftware so einzurichten, dass sie einem Lieferanten eine automatische E-Mail schickt, wenn zum Beispiel der Toner fast leer ist. So müssen sich Administratoren weniger Gedanken um diese Standardaufgabe machen.

Fazit

Eine intelligente Netzwerk-Monitoring-Lösung bietet dem Administrator Hilfestellung bei den Herausforderungen seines Arbeitsalltags. Sie steht dem IT-Verantwortlichen als ausfallsicherer und umfassender Helfer rund um die Uhr zur Seite. Durch die Überwachung aller Netzwerkkomponenten und sogar der Umgebungsparameter des Serverraums gibt die Software der IT-Abteilung ein sicheres Gefühl. Probleme werden schnell erkannt, umgehend gemeldet und können zügig behoben werden, bevor wirklicher Schaden entsteht.

Gerald Schoch