

# Kriterien für die Auswahl einer geeigneten Netzwerk-Monitoring-Lösung

Whitepaper

Kriterien für die Auswahl einer geeigneten Netzwerk-Monitoring-Lösung

## Inhalt

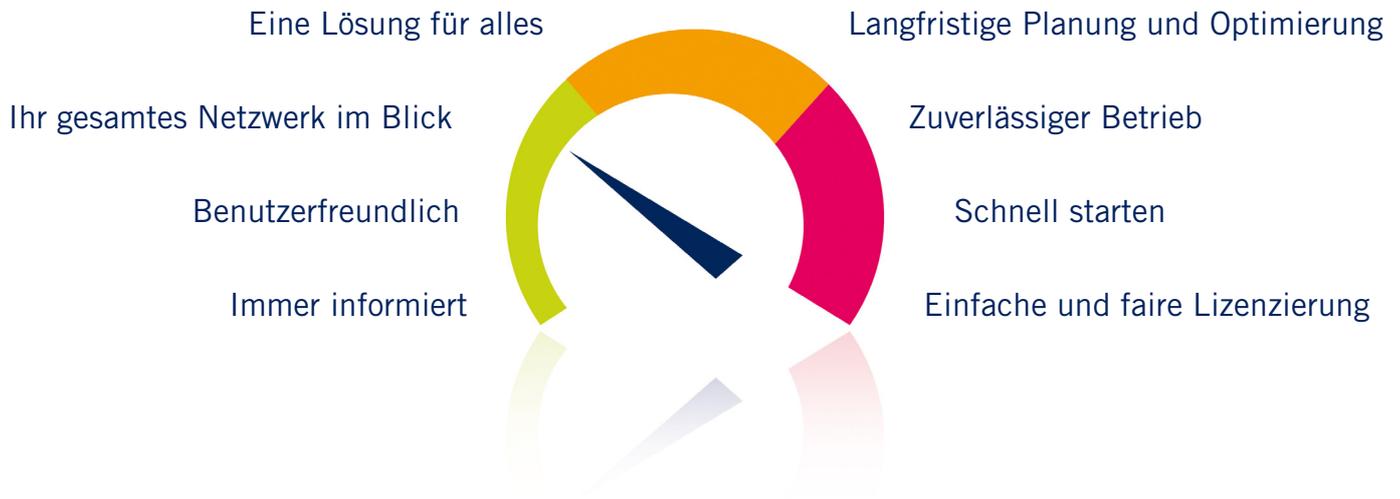
Einleitung.....	3
Warum Netzwerk-Monitoring? .....	4
Mehr Zeit für Wesentliches .....	4
Plus an Sicherheit .....	4
... Kontrolle ist besser .....	5
Potenzial steigern .....	5
Finanzielle Einsparungen .....	5
Klassifizierungen von Netzwerk-Monitoring-Lösungen .....	6
Open Source-Software .....	6
Einstiegs-Monitoring-Lösungen .....	6
„Spezialisten“ .....	6
Enterprise-Netzwerkmanagement-Software .....	6
„All-in-One“-Monitoring-Lösung .....	7
Auswahlkriterien für eine geeignete Netzwerk-Monitoring-Lösung .....	7
Stichwort Vereinfachung .....	7
Die Anforderungen kennen .....	8
Technische „Must-Haves“ .....	9
Vorzüge in puncto Handhabung und Service .....	10
Zusammenfassung .....	10
Checkliste zur Auswahl einer Netzwerk-Monitoring-Software .....	11

### Einleitung

Ein hoch performantes Netzwerk gehört heutzutage zu den Grundvoraussetzungen für jede funktionierende IT-Infrastruktur in Unternehmen. Um einen reibungslosen Geschäftsablauf zu sichern, sollten alle Prozesse ohne Komplikationen ablaufen; ebenso wie die interne und externe Kommunikation zwischen verschiedenen Firmenstandorten bzw. mit Kunden und Partnern. Störungen und Ausfälle in den betrieblichen Abläufen schlagen sich schnell in zeitlichen und vor allem finanziellen Verlusten nieder. Um Verfügbarkeit, Performance sowie Bandbreitenauslastung in einem IT-Netzwerk stets im Blick zu behalten, empfiehlt sich der Einsatz eines Netzwerk-Monitoring-Systems, das permanent die Vorgänge im Netzwerk überwacht, analysiert und das IT-Personal alarmiert, sobald Fehler auftreten oder kritische Werte überschritten werden. Auf diese Weise ermöglicht Netzwerk-Monitoring dem Administrator ein zeitnahes Eingreifen, ggf. auch per Remote-Verbindung, falls er nicht vor Ort ist.

Allerdings stellt jedes Unternehmen unterschiedliche Anforderungen an eine Netzwerküberwachungslösung, und da der Markt mittlerweile zahlreiche unterschiedliche Tools und Lösungen anbietet, ist eine sorgfältige Vorauswahl ratsam. Dieses Whitepaper zeigt auf, welche Möglichkeiten Netzwerk-Monitoring bieten kann, wenn bei der Auswahl der Lösung die richtigen Kriterien in die Entscheidungsfindung einfließen.

## Warum Netzwerk-Monitoring?



Immer mehr Unternehmen integrieren mittlerweile eine Netzwerküberwachungslösung in ihr IT-Konzept. Die Rund-um-die-Uhr-Überwachung zahlt sich in vielen Bereichen aus: So sorgt sie unter anderem für eine enorme Zeitersparnis und unterstützt die Administratoren bei der Planung von Ressourcen sowie der Optimierung des Unternehmensnetzwerkes.

### Mehr Zeit für Wesentliches

Generell zeichnet sich eine Monitoring-Lösung durch frühzeitiges Erkennen und Melden von Fehlern, Störungen und überschrittenen Grenzwerten aus und ermöglicht so ein sofortiges Eingreifen. Zudem muss das IT-Personal nicht mehr kontinuierlich alle Netzwerkkomponenten wie Server, Desktop-Rechner, Applikationen, Traffic und mehr aktiv im Auge behalten. Dadurch spart ein Monitoring-System gleich zweifach wertvolle Zeit ein, die die Administratoren sinnvoll für andere Aufgaben einsetzen können. Dies unterstreicht auch aktuell eine Kundenumfrage der Paessler AG: 90 % der 724 befragten Kunden gaben an, dass sie durch den Einsatz der Netzwerküberwachungslösung PRTG Network Monitor deutlich Zeitressourcen einsparen: 43 % erzielen pro Woche rund drei Stunden eingesparte Arbeitszeit.

### Plus an Sicherheit

Auch in Hinblick auf das Thema Sicherheit leistet eine Monitoring-Lösung einen wertvollen Beitrag. Meldet sie z.B. eine plötzlich auftretende hohe CPU-Belastung oder weicht der Traffic ungewöhnlich stark von den üblichen Werten ab, kann das für die IT-Mitarbeiter ein wichtiger Hinweis auf mögliche Malware- oder Phishing-Angriffe sein. Eine Netzwerküberwachungs-Software lässt sich unkompliziert in ein bestehendes Security-Konzept mit Virenschannern, Firewalls usw. integrieren, um den Schutz weiter zu erhöhen.

## Kriterien für die Auswahl einer geeigneten Netzwerk-Monitoring-Lösung

### ... Kontrolle ist besser

Durch das umfassende Monitoring der gesamten Netzwerklandschaft sowie die sofortigen Alarme bietet eine Netzwerk-Monitoring-Lösung dem IT-Personal mehr Kontrolle über dessen Aufgabenbereich. Denn das IT-Team hat das Netzwerk jederzeit im Auge und somit einen tiefen Einblick in die aktuellen Vorgänge im Netzwerk sowie über die Auslastung der einzelnen Ressourcen. Der aktuelle Status sowie weitere Detailinformationen können jederzeit eingesehen werden. Da einige Lösungen einen Remote-Zugang oder Smartphone-Apps bereitstellen, kann sich der Administrator sogar dann um sein Netzwerk kümmern, wenn er nicht vor Ort ist. Dieser Überblick senkt den Stressfaktor für die gesamte IT-Abteilung: Solange kein Alarm ausgelöst wird, ist davon auszugehen, dass alles fehlerfrei funktioniert.

### Potenzial steigern

Mit Hilfe der umfangreichen Datensammlungen, die die Netzwerk-Monitoring-Software anlegt, lassen sich zuverlässige Trendanalysen erstellen. So gewinnen IT-Verantwortliche einen tieferen Einblick in ihr Netzwerk und können Optimierungspotenzial rechtzeitig aufdecken und nutzen. Beispielsweise hilft die Ermittlung des tatsächlichen Bandbreitenbedarfs dabei, die zur Verfügung stehenden Ressourcen gezielter planen und einsetzen zu können, was besonders für Virtualisierungsprojekte ein wichtiger Faktor ist. Darüber hinaus kann der Administrator auf dieser Basis die Einhaltung der Service Level Agreements (SLAs) sicherstellen.

Die Einhaltung der SLAs kann durch die richtige Netzwerk-Monitoring-Software sichergestellt werden.

### Finanzielle Einsparungen

Da professionelle Netzwerk Monitoring-Systeme mit großem Funktionsumfang bereits zu überschaubaren Preisen angeboten werden, belasten sie das Budget der IT-Abteilung nur gering, bieten aber ein hohes Potenzial, um Zeit und Ressourcen einzusparen. Nicht zuletzt beugen sie auch großen wirtschaftlichen Schäden durch zu spät erkannte Ausfälle vor. Bei der Auswahl sollte darauf geachtet werden, dass der Hersteller ein möglichst transparentes Lizenzmodell anbietet. So ist der Anwender davor gefeit, weitere benötigte Funktionen als separates Paket dazukaufen zu müssen.

Mit einer professionellen Monitoring-Lösung können Zeit und Ressourcen eingespart werden.

Netzwerk-Monitoring-Lösungen sorgen durch zeitnahe Fehlermeldungen für schnelle Reaktions- und somit keine oder nur geringe Ausfallzeiten. Mit der Analyse des tatsächlichen Netzwerkzustandes ist es dem IT-Personal möglich, Schwachstellen oder Verbrauchsspitzen auszumachen und diese entsprechend zu regeln, abzuschalten oder zu ersetzen, bevor sie zu gravierenden Beeinträchtigungen des Geschäftsablaufs führen.

„Richtig tolle Software!!! Früher haben wir einen Nagios zusammengeflickt und eher mehr Zeit in die Einstellungen selbst investiert als in die Überlegungen... SMS Alarmierung hat uns damals einen Arbeitstag gekostet. PRTG hat es alles mit 5 Klicks. Wir stehen auch schon mit den Sensoren „kurz vor dem Upgrade“ da PRTG so viel Sinn und Spaß macht.“

Simon Pucher, Geschäftsführer & IT Leiter bei der e-derm-consult GmbH

### Klassifizierungen von Netzwerk-Monitoring-Lösungen

Jedes Unternehmen und damit auch jedes Netzwerk stellt andere Anforderungen an eine Monitoring-Software. Aus diesem Grunde entwickelten sich zahlreiche Lösungen, die diese Bedürfnisse möglichst optimal abdecken wollen. Allerdings ist dadurch der Markt mittlerweile recht unübersichtlich geworden. In einer groben Einteilung lassen sich jedoch vier Typen unterscheiden.

#### Open Source-Software

Angesichts oft schmaler Budgets für IT-Abteilungen setzen einige Unternehmen auf Open Source-Software, in der vermeintlichen Hoffnung, schnell eine kostengünstige Lösung einrichten zu können. Da sich diese Systeme in der Regel individuell anpassen lassen und lizenzkostenfrei nutzbar sind, bieten sie auf den ersten Blick viele Vorteile. Allerdings überwiegen bei genauerem Hinsehen sehr oft die Nachteile. Der überdurchschnittliche Aufwand für Implementation und Konfiguration und vor allen Dingen der oft eingeschränkte Funktionsumfang sind nicht zu vernachlässigende Mankos. Meist sind nur Basisfunktionen integriert, die nicht in der Lage sind, Netzwerke detailliert zu überwachen. Ein weiteres Problem stellt das Fehlen eines verantwortlichen Herstellers dar: Produktsupport erfolgt in der Regel durch die Community und ist entsprechend unzuverlässig, so dass der Anwender bei Fragen oder Problemen meist auf sich gestellt ist.

In der Regel individuell anpassbar und lizenzkostenfrei, aber überdurchschnittlicher Aufwand für Implementation und Konfiguration.

#### Einstiegs-Monitoring-Lösungen

Wer ein ernsthaftes Interesse daran hat, sein Netzwerk langfristig und vor allem zuverlässig zu überwachen, kann im ersten Schritt auf kostengünstige Einstiegslösungen zurückgreifen. Zwar bieten auch diese keinen vollwertigen Funktionsumfang, aber zumindest eine Basis-Bandbreitenüberwachung mittels SNMP oder eine Kontrolle der Verfügbarkeit via Ping. Auf Grund des reduzierten Umfangs eignet sich derartige Software eher für kleinere Netzwerke bzw. für den Einstieg ins Monitoring. Falls die Überwachung ausgeweitet werden soll, bleibt nur der Umstieg auf eine Lösung, die größere Kapazitäten und eine umfangreichere Überwachung erlaubt.

Kostengünstige Einstiegs-Lösungen bieten zwar keinen vollwertigen Funktionsumfang, aber zumindest eine Basisüberwachung.

#### „Spezialisten“

In diese Gruppe fallen Monitoring-Systeme, die auf spezifische Bereiche innerhalb des Netzwerkes ausgerichtet sind, wie z.B. die Bandbreitenmessung mittels Packet Sniffing. Durch die Spezialisierung sind sie in ihrem Gebiet hoch performant, auf der anderen Seite jedoch nicht für ein breit angelegtes Monitoring geeignet. „Spezialisten“ werden in der Regel von ebenso spezialisierten Unternehmen zur Überwachung von Hochleistungsleitungen oder Netzwerken eingesetzt; meist in Kombination mit breiter aufgestellten Lösungen als Ergänzung.

Ausrichtung liegt auf spezifischen Bereichen wie Bandbreitenmessung mittels Packet Sniffing.

#### Enterprise-Netzwerkmanagement-Software

Bei Enterprise-Netzwerkmanagement-Lösungen sind Monitoring-Systeme meist nur ein Baustein innerhalb eines wesentlich umfangreicheren Konzepts. Auf Grund hoher Lizenzkosten und aufwendiger Installationen sind sie für mittelständische Unternehmen zumeist nicht von Interesse. Dazu kommt, dass diese Systeme nicht auf den Bereich Netzwerk-Monitoring fokussiert sind und in puncto Funktionalität und Usability nicht mit eigenständigen Netzwerk-Monitoring-Lösungen mithalten können.

Das Monitoring-System ist meist nur ein Baustein innerhalb eines wesentlich umfangreicheren Konzepts. Dadurch entstehen hohe Kosten und eine aufwendige Installation.

Kriterien für die Auswahl einer geeigneten Netzwerk-Monitoring-Lösung

„All-in-one“-Monitoring-Lösungen

Der Trend in den vergangenen Jahren geht hin zu „All-in-one“-Lösungen

Aufgrund der wachsenden Bedeutung einer professionellen Netzwerküberwachung geht der Trend in den vergangenen Jahren hin zu „All-in-one“-Netzwerk-Monitoring-Software. Sie bietet sowohl verschiedene generelle Überwachungsfunktionen als auch spezielle Features für einzelne Teilbereiche. Beispielsweise beherrschen diese Lösungen die herkömmlichen Protokolle wie SNMP, Packet Sniffing sowie Flow-Protokolle zur Bandbreitenüberwachung. Außerdem stellen sie in den meisten Fällen bereits eine breite Auswahl an weiteren Überwachungssensoren und Protokollen zur Verfügung (SQL, FTP, HTTP, Exchange, POP3, virtuelle Server etc.). Derartige Produkte lassen sich in der Regel unkompliziert und in kurzer Zeit installieren. Außerdem verfügen sie meist über einen professionellen und zuverlässigen Hersteller-Support. Ein weiteres Plus: Bei Bedarf lassen sich die Lösungen durch skalierbare Lizenzen an wachsende Netzwerkstrukturen anpassen, und die Anschaffungskosten sind überschaubar. Dennoch reicht die Preisspanne von 500 € bis hin zu 50.000 € und mehr – ein Grund mehr, die tatsächlichen Anforderungen innerhalb des Unternehmens genau zu analysieren, um keine unnötigen Investitionen zu tätigen.

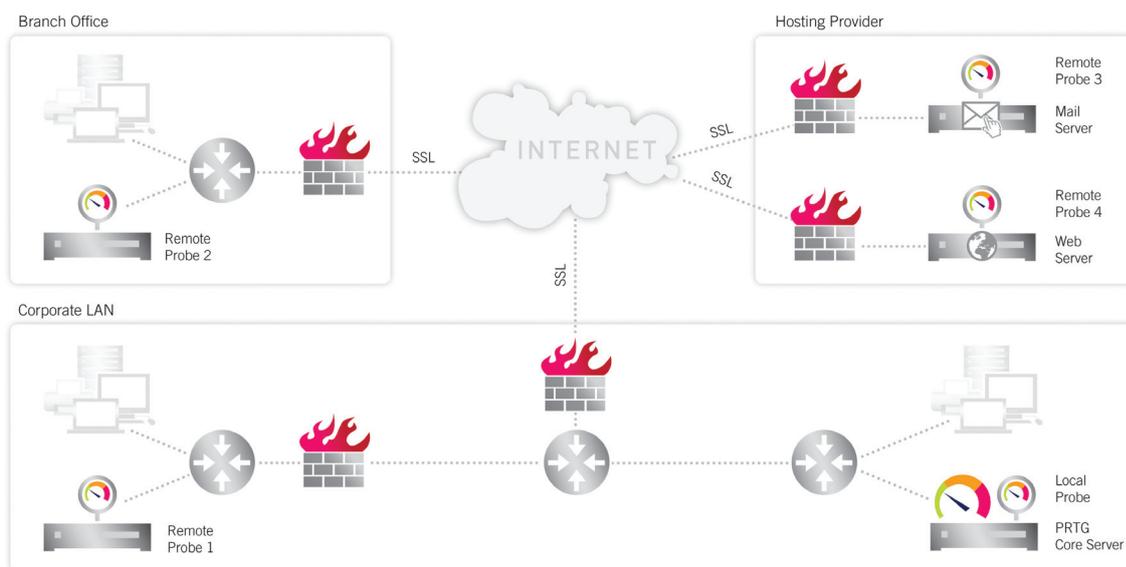


Abbildung: Eine Lösung für die Überwachung der gesamten, auf mehrere Netzwerke verteilten Unternehmens-IT.

Auswahlkriterien für eine geeignete Netzwerk-Monitoring-Lösung

In die Entscheidungsfindung sollten neben den Kosten einige grundlegende Faktoren einfließen, die sowohl die gegebene Infrastruktur als auch die jeweiligen Eigenschaften einer potenziellen Lösung berücksichtigen. Die Verantwortlichen müssen sich vor allem im Klaren darüber sein, welche Anforderungen sie an das System stellen und für welche Einsatzgebiete es gedacht ist.

Stichwort Vereinfachung

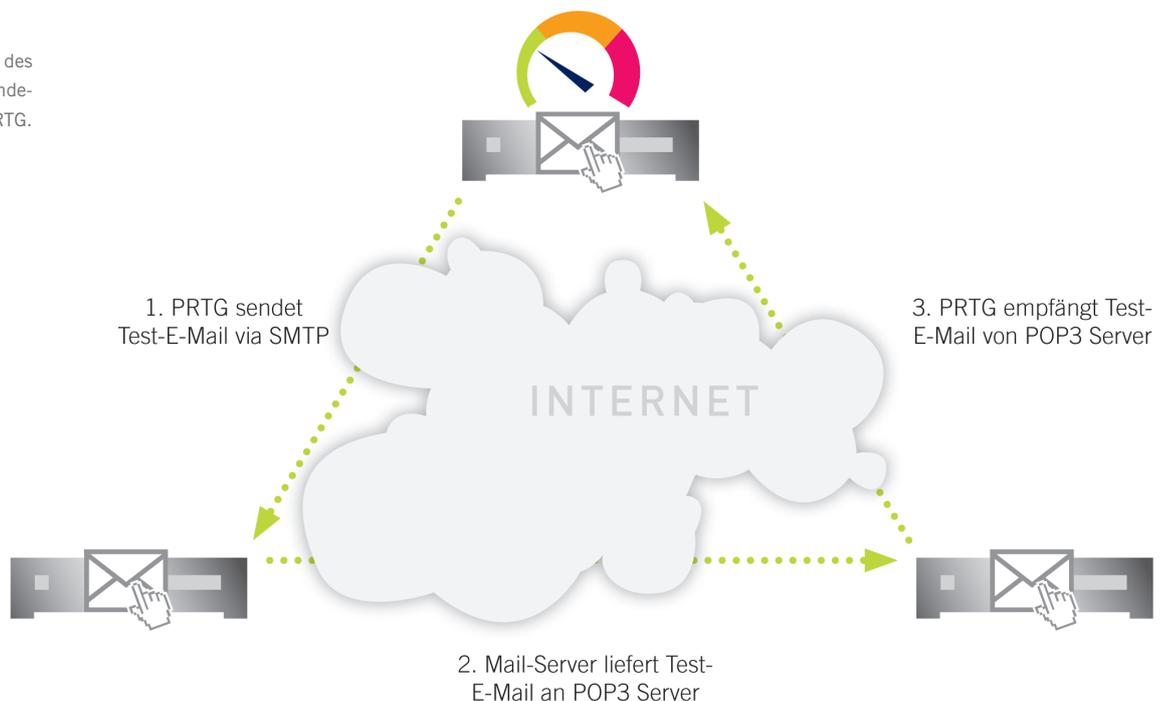
Grundsätzlich sollte eine Network Monitoring-Software dafür sorgen, dass der Administrator Zeit für andere sinnvolle Aufgaben erhält, statt permanent die Infrastruktur mit allen angeschlossenen Systemen im Auge behalten zu müssen. Oder anders ausgedrückt: Nach einer unkomplizierten Installation arbeitet die Lösung selbsttätig, sodass sie keine Mehrarbeit für das IT-Personal darstellt, sondern Freiräume schafft.

Kriterien für die Auswahl einer geeigneten Netzwerk-Monitoring-Lösung

Die Anforderungen kennen

Die Wahl eines geeigneten Network Monitoring-Systems richtet sich zum einen grundsätzlich nach der Größe des zu überwachenden Netzwerkes, zum anderen spielen die zu kontrollierenden Instanzen eine Rolle. Dazu zählen beispielsweise Server, Switches, Arbeitsplatzrechner sowie die Verbindungen zwischen diesen und die Anbindung an Außenstandorte und das Internet. Zwei wichtige Bereiche, die vermutlich in jedem Unternehmen überwacht werden sollten, sind die Website und die E-Mail-Kommunikation. Bei Ersterer ist es sinnvoll, nicht nur die reinen Antwortzeiten, sondern die generelle Performanz wie auch die einzelner Komponenten wie z.B. eines Shops oder von Formularen zu überwachen. Gerade bei international agierenden Firmen ist ein Monitoring-System eine große Hilfe dabei, die Antwortzeiten für Anfragen aus verschiedenen Ländern zu überprüfen und ggf. zu optimieren. In puncto E-Mail-Verkehr unterstützt eine Überwachungssoftware die IT-Abteilung dabei, die Verfügbarkeit der POP3- und IMAP-Server zu beobachten. Ebenso hilft sie, Störungen bei der Zustellung aufzudecken, indem sie via Test-Mails den gesamten Zustellvorgang analysiert, vom Senden einer E-Mail bis zum Eingang beim Empfänger.

Abbildung: Überwachung des kompletten E-Mail Versende-Zyklus mit PRTG.



Auf Grund noch fehlender Monitoring-Erfahrung werden im Voraus oftmals zu geringe Einsatzmöglichkeiten identifiziert. Außerdem wachsen Netzwerke und damit der Monitoring-Bedarf. Daher ist es von Vorteil, eine Lösung zu wählen, die bei Bedarf „mitwachsen“ kann. Um Unsicherheiten schon vor dem Kauf zu klären, sollte dem Anwender eine Testversion mit allen Funktionen zur Verfügung stehen, die er nach erfolgreichen und zufriedenstellenden Probeläufen als produktive Lösung kaufen und ohne Unterbrechung oder Neuinstallation übernehmen kann. Sollte es beim Einsatz des Testsystems zu Problemen kommen, ist dies auch der richtige Zeitpunkt, um die Qualität des Herstellersupports zu testen, damit der Produktivbetrieb dann so weit wie möglich komplikationsfrei verläuft.

Kriterien für die Auswahl einer geeigneten Netzwerk-Monitoring-Lösung

Technische „Must-Haves“

Zu den Kernelementen bezüglich technologischer Voraussetzungen der Monitoring-Lösung zählen die Bandbreiten-, Auslastungs- und Verfügbarkeitsüberwachung. Hierbei ist besonders auf eine breit angelegte Unterstützung der bekanntesten Protokolle und Technologien wie z.B. WMI, NetFlow, sFlow, jFlow, Packet Sniffing und SNMP zu achten, denn meist sind Netzwerke äußerst heterogene IT-Landschaften. Durch die Abdeckung der gängigsten Protokolle ist ein umfassendes Monitoring möglich. Ebenfalls von Vorteil ist es, eine optionale Remote-Überwachung für mehrere Standorte bzw. Netzwerke zur Verfügung zu haben. Manchmal ist diese schon Bestandteil des jeweiligen Leistungspaketes bzw. der Lizenz.

Aus den gesammelten Leistungsdaten bezüglich Bandbreite und Verfügbarkeit fertigt eine gute Netzwerküberwachungs-Software übersichtliche und detaillierte Graphen, Berichte sowie Listen an, die dem Administrator schnell Informationen zur Verfügung stellen. Darüber hinaus archiviert sie alle Daten, sodass die IT-Mitarbeiter einen Langzeitüberblick gewinnen und an Hand von erkennbaren Trends und Lastspitzen Verbesserungen bzw. Veränderungen vornehmen können. Damit ist die Basis für ein professionelles Netzwerkmanagement gegeben.

Eine wichtige Funktion zur Entlastung des IT-Personals sind Alarmer, die dem zuständigen Administrator melden, wenn Störungen vorliegen, voreingestellte Schwellenwerte erreicht bzw. überschritten sind oder Geräte ausfallen. Bei den meisten Lösungen lassen sich solche Alarmer bedarfsgerecht anpassen, sodass sie den Administrator per E-Mail, SMS-/Pager-Benachrichtigung, Syslog, HTTP Request erreichen oder aber über ausführbare .exe-Dateien das Problem direkt selbst beheben können. Dies verschafft dem zuständigen Personal mehr Sicherheit und Ruhe. Außerdem sollten für Alarmer Abhängigkeiten definiert werden können: Dadurch meldet die Lösung z.B. einen Serverausfall, aber die Applikationen, die an diesen Server angebunden sind, erzeugen keine weiteren, eigenständigen Meldungen. So entsteht keine unübersichtliche Flut von redundanten Meldungen.

Für mehr Sicherheit im Hinblick auf mögliche Ausfälle der Monitoring-Software sorgt eine integrierte Cluster-Funktion. Mit Hilfe dieses Features erfolgt die Überwachung parallel durch mehrere Instanzen der Software. Fallen eine oder mehrere dieser Instanzen aus, übernehmen die noch funktionstüchtigen deren Aufgaben und setzen das Monitoring unterbrechungsfrei fort. Auf diese Weise ist der Anwender vor Ausfällen der Software geschützt und kann die Performanz des Netzwerkes besser sicherstellen.

Im Zuge des sich immer weiter verbreitenden Cloud Computing-Konzepts und des vermehrten Einsatzes virtualisierter Systeme sollte die Netzwerk Monitoring-Lösung auch entsprechende Möglichkeiten zur Überwachung dieser Systeme bieten. Hier ist eine Auswahl aus verschiedenen Sensortypen von Vorteil, die speziell für den Einsatz in virtuellen Umgebungen konzipiert sind, z.B. für VMware, Microsoft Hyper-V, Parallels Virtuozzo Container oder Amazon Elastic Compute Cloud (EC2).



Abbildung: Der Sunburst View von PRTG bietet einen schnellen Überblick über den Zustand des Netzwerks.

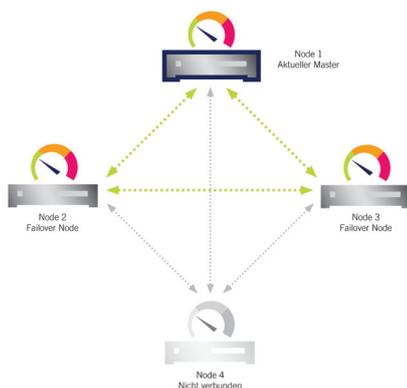


Abbildung: Die in PRTG integrierte Cluster Funktion stellt ein unterbrechungsfreies Monitoring sicher.

Kriterien für die Auswahl einer geeigneten Netzwerk-Monitoring-Lösung

Vorzüge in puncto Handhabung und Service

Selbstverständlich sollte eine Network Monitoring-Software benutzerfreundlich aufgebaut sein, mit klar verständlichen Menüs und intuitiver Bedienmöglichkeit. Darüber hinaus muss die Benutzeroberfläche flexibel gestaltet und beispielsweise als Windows-, Web- und Mobile-Interface zu verwenden sein. In der Regel gehört auch eine automatische Netzwerkerkennung nach der Installation zum Standard. Angenehm, aber nicht unbedingt Voraussetzung, ist eine Lösung in Landessprache.

Abbildung: Verschiedene Benutzeroberflächen erlauben sowohl direkten als auch Remote-Zugriff.



Bei der Arbeit mit Grafiken und Berichten profitieren Administratoren davon, wenn sie Aufbau und Gestaltung an ihre individuellen Bedürfnisse anpassen und so beispielsweise auf häufig benötigte Analysen schneller zugreifen können. Zumeist lassen sich die einzelnen Geräte auch zu Gruppen zusammenfassen, was für mehr Übersicht sorgt. Manche Lösungen bieten für den Einstieg bereits vorgefertigte Templates für einen Überblick über die Soft- und Hardware-Komponenten an, die dann nach Bedarf konfiguriert werden können. Optional kann das IT-Personal hier zwischen einer Zusammenfassung und einer Detailansicht wählen.

Bevor eine finale Entscheidung für ein bestimmtes Monitoring-System fällt, sollte das Unternehmen im letzten Schritt die Konditionen genau unter die Lupe nehmen. Hier sind die Hersteller interessant, deren einfach strukturierte Lizenzierungsmodelle ohne versteckte Nebenkosten für Transparenz sorgen. Ebenfalls ein Pluspunkt sind integrierte Upgrade-Optionen, falls das Netzwerk erweitert wird – so sind Unternehmen für zukünftige Aufgaben gerüstet. Weitere Pluspunkte kann eine Monitoring-Lösung sammeln, für die ein Support seitens des Herstellers sowie weiterführende Informationen in Form von Handbüchern etc. in der jeweiligen Landessprache vorhanden sind.

Zusammenfassung

Eine Network Monitoring-Lösung stellt eine sinnvolle Ergänzung der Netzwerkinfrastruktur dar und sorgt zum einen für eine Entlastung der IT-Abteilung sowie zum anderen für die Aufdeckung bislang unerkannter Optimierungsmöglichkeiten. Allerdings kann sie ihr volles Potenzial nur dann entfalten, wenn sie auf die Anforderungen des Netzwerkes abgestimmt ist. Daher sollten sich Unternehmen bei der Suche nach dem passenden System ausreichend Zeit zum Testen und Vergleichen nehmen, ohne direkt die erstbeste Lösung zu kaufen. Die folgende Checkliste führt die wichtigsten Kriterien bzw. im Vorhinein zu klärende Fragen noch einmal auf.

### Checkliste zur Auswahl einer Netzwerk-Monitoring-Software

- Was muss das Monitoring-System leisten können? Wie groß ist das bestehende Netzwerk? Gibt es schon konkrete Pläne für Erweiterungen, die in die Planung mit einbezogen werden müssen? Ist die Lösung durch Upgrade-Möglichkeiten zukunftssicher?
- Soll ein umfassendes Monitoring erfolgen, oder sollen nur bestimmte Bereiche speziell überwacht werden?
- Gibt es eine Testversion, die im besten Falle bei erfolgreichem Einsatz mit allen vorgenommenen Installationen direkt im Produktivbetrieb verbleiben kann?
- Welche Protokolle und Technologien unterstützt die Lösung bezüglich Bandbreiten- und Verfügbarkeitsüberwachung? Reichen diese für die Anforderungen des Unternehmens aus? Gibt es die Möglichkeit zur zentralen Überwachung verteilter Standorte?
- Welche Daten sammelt die Lösung? Wie werden sie ausgewertet? Lassen sich die Grafiken, Berichte etc. anpassen? Gibt es ein langfristiges Datenarchiv und damit die Möglichkeit einer Trendanalyse?
- Über welche Wege alarmiert die Lösung den/die Verantwortlichen im Notfall? Lassen sich diese Wege konfigurieren?
- Ist die Lösung benutzerfreundlich gestaltet? Lässt sie sich intuitiv bedienen? Sind Einstellmöglichkeiten (bspw. individuelle Oberflächen) vorhanden? Ist das Interface so ausgelegt, dass es auf dem Betriebssystem, im Browser und auf mobilen Geräten funktioniert?
- Ist die Lösung in der Landessprache verfügbar? Gibt es entsprechenden Support von Seiten des Herstellers? Stehen weitere Informationsquellen wie Handbücher, Blogs und/oder Foren zur Verfügung?
- Wie transparent ist die Preispolitik des Herstellers? Passen die Lizenzierungsmodelle zu den Anforderungen des Unternehmens?

#### Über die Paessler AG

Die Paessler AG mit Sitz in Nürnberg entwickelt Software für die Bereiche Netzwerküberwachung und Webserveranalyse seit 1997. Weltweit setzen mehr als 150.000 Administratoren, Webseitenbetreiber, Internet Service Provider und andere IT-Verantwortliche Paessler Software ein. Freeware und Testversionen aller Produkte können unter [www.de.paessler.com](http://www.de.paessler.com) heruntergeladen werden.

##### Paessler AG

Bucher Straße 79a, 90419 Nürnberg, Deutschland  
[www.paessler.com](http://www.paessler.com), [info@paessler.com](mailto:info@paessler.com)

UST#: DE 217564187

Steuer#: FA Nürnberg 241/120/60894

Eintragung: Amtsgericht Nürnberg HRB 23757

Vorstand: Dirk Paessler, Christian Twardawa

Vors. d. Aufsichtsrats: Dr. Marc Rössel

