Netzvisualisierung

Monitoring zur Netzdokumentation nutzen

Kai-Oliver Detken

Die IT-Infrastruktur muss heute eine Verfügbarkeit von nahezu 100 % besitzen. Das gilt insbesondere, seit ebenfalls die Telefonie (Stichwort VoIP) über sie abgewickelt wird. Um dies sicherstellen zu können, sind Monitoring-Systeme unabdingbar, die den Status von Diensten und Serversystemen permanent überprüfen. Allerdings ist die Pflege oftmals aufwendig, so dass die Motivation eines IT-Administrators mit dem Aufwand exponenziell abnimmt. Einfache Pflegbarkeit ist also ein wichtiger Aspekt sowie die kontinuierliche Dokumentation des Unternehmensnetzes, die auch gesetzlich gefordert wird. Beide Anforderungen lassen sich realisieren, wenn man das richtige Monitoring einsetzt.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Aufgrund der Notwendigkeit von hochverfügbaren Netzdiensten existieren bereits seit einigen Jahrzehnten Monitoring-Systeme, die auf die Überwachung von IT-Systemen und -Infrastrukturen spezialisiert wurden. Setzte man anfangs stark auf spezielle Herstellersysteme wie z.B. HP OpenView oder IBM Tivoli, die allerdings auf die jeweiligen Herstellerkomponenten fokussiert waren, kamen später auch Open-Source-Systeme wie Nagios zum Einsatz, die alle aktiven Komponenten eines Netzes einbinden konnten. Während die proprietären Systeme optimal mit den eigenen Komponenten zusammenspielten und dadurch auch die Einbindung erleichterten, zeichnete sich Nagios eher durch Lizenzkostenfreiheit und Herstellerunabhängigkeit aus anstatt durch leichte Handhabbarkeit. Auch bez. der Skalierbarkeit setzte Nagios Grenzen, so dass es entsprechend in Forks weiterentwickelt wurde. Trotzdem setzten sich Nagios oder dessen Derivate in Unternehmensnetzen durch, was hauptsächlich daran lag, dass man alle aktiven Komponenten einbinden konnte und nicht auf einen Hersteller festgelegt war.

Folgende Nagios-Varianten lassen sich nennen (s. a. NET 5/2016, S. 33):

- Nagios: modular aufgebaute Software, bestehend aus dem Nagios-Kern und externen Programmen, sog. Plugins, die die Überwachung von Hosts und deren Diensten durchführen;
- Icinga: Fork von Nagios, der von einer deutschen Community im Jahr 2009 unter Beibehaltung der Kompatibilität zu Nagios gestartet wurde; zeichnet sich insbesondere durch zusätzliche Datenbankkonnektoren (z.B. für MySQL und PostgreSQL) und die moderne Weboberfläche aus; Letztere ist in unterschiedlichen Varianten (Icinga Classic, Icinga 2) nutzbar und bindet mobile Endgeräte sehr gut als Anzeigemöglichkeit mit ein; Plugins von Nagios lassen sich auch bei Icinga nutzen;
- Check_MK: wurde ursprünglich im Jahr 2008 als Addon für Nagios zur deutlichen Steigerung von Performance und damit Skalierbarkeit entwickelt; löst sich inzwischen immer mehr von Nagios, indem ein eigener, eigenständig nutzbarer Micro Core realisiert wurde.

Als proprietäres Monitoring-System, das ebenfalls auf keiner Herstellerlösung basiert, kann noch der InterMapper genannt werden. Alle diese Systeme eignen sich neben der Überprüfung der Verfügbarkeit auch zur Visualisierung der IT-Infrastruktur.

Netzvisualisierung

Neben Warnmeldungen, die permanent über den Gesundheitszustand des Netzes Auskunft geben, sind alle diese Monitoring-Systeme in der Lage, die jeweilige Netztopologie abzubilden und damit die IT-Infrastruktur greifbarer und dokumentierbar zu machen. Besonders übersichtlich schafft dies der InterMapper der amerikanischen Firma Helpsystems (*Bild 1*). Mit ihm lassen sich große Provider-Netze abbilden und z.B. in unterschiedliche Schichtenstrukturen überführen. Dies ist auch der Grund, weshalb der InterMapper bei Internet Service Providern (ISP) häufig eingesetzt wird.

Ein weiterer Vorteil der InterMapper-Ansicht ist, dass das Netz in Echtzeit angezeigt werden kann, d.h., man erkennt, mit welcher Datenrate die Netzkomponenten verbunden sind, ob Daten auf diesen Leitungen ausgetauscht werden oder welche Dienste eine Zeit lang nicht verfügbar waren. Nicht funktionierende Komponenten werden rot dargestellt, während Verletzungen bestimmter Randparameter (z.B. Festplattenkapazität wurde nahezu erreicht) durch orange angezeigt werden. Das Ziel sollte es dabei sein,

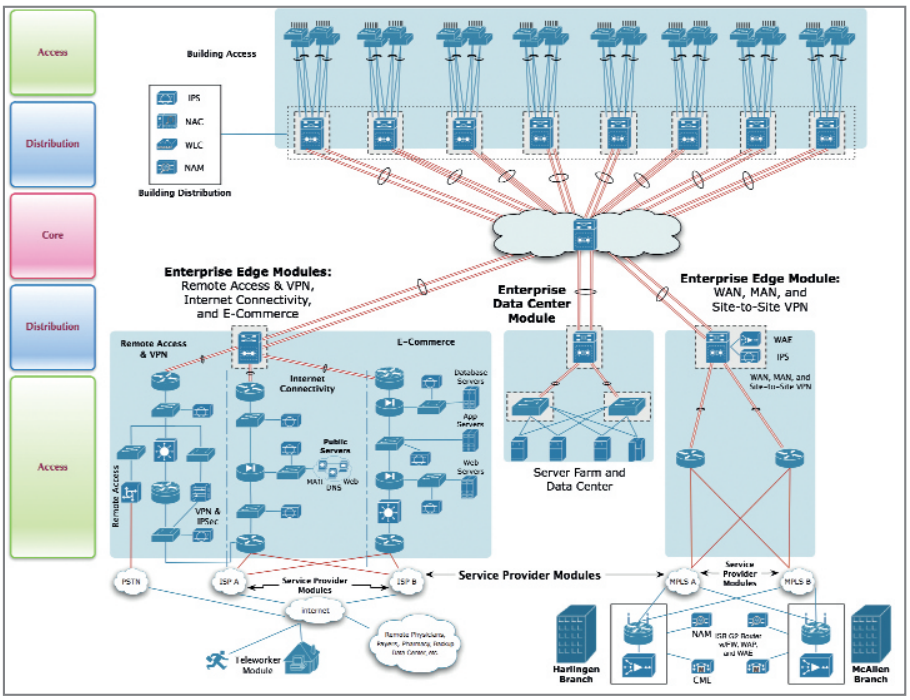

Bild 1: Strukturierte Netzdarstellung mithilfe von InterMapper

dass alle Komponenten möglichst den Status grün nie verlassen. Tun sie es doch einmal, erhält der Administrator eine entsprechende E-Mail oder SMS.

Eine Inventarisierung vorhandener Komponenten ist dadurch ebenfalls indirekt möglich, da der Administrator automatisch neue Serversysteme, Firewalls, Speichereinheiten usw. mit in das Monitoring aufnimmt. Dies sollte er schon aus Eigeninteresse tun, da er so schneller auf etwaige Störungen reagieren und die Geschäftsleitung auch einfacher auf Missstände hinweisen kann.

Im Übrigen sind auch Nagios und Icinga in der Lage, Netztopologien darzustellen. Aber sie sind weder interaktiv, noch so übersichtlich wie beim InterMapper (*Bild 2*).

Diese Darstellungsweise hilft natürlich auch bei einer notwendigen Netzdokumentation, die in Unternehmen oft vernachlässig wird. Denn frühere Bestrebungen, die Netzstruktur mithilfe von Zeichen-Tools wie Visio aufzubereiten, hatten den Nachteil, dass man immer nur einen bestimmten Zeitpunkt dokumentieren konnte. Jede Änderung der Infrastruktur hätte sofort manuell nachgezogen werden müssen, was aber aus Zeitgründen nicht gemacht wurde. Dementsprechend waren keine oder völlig veraltete Dokumentationen an der Tagesordnung. Man sprach in diesem Fall auch vom sog. Turnschuh-Administrator, der erst tätig wurde, wenn ein Anwender einen Ausfall meldete und der danach die defekte IT-Komponente mühsam suchen musste.

Hinzu kommt, dass immer mehr Unternehmen sich ISO-Zertifizierungen unterziehen, die IT-Audits zur Pflicht werden lassen. In diesen Audits wird auch die Netzdokumentation einer genauen Prüfung unterzogen, ohne die kein Audit bestanden werden kann. Darunter fallen auch testierte Jahresabschlüsse durch einen Wirtschaftsprüfer, die ebenfalls Backup- und ERP-Systeme mit einbeziehen müssen und daher auch auf die Dokumentation der gesamten Umgebung Wert legen. Letzteres betrifft auch zunehmend kleine und mittlere Betriebe (KMU), die bisher davon ausgegangen waren, dass IT-Dokumentation zu aufwendig ist bzw. nur Ressourcen und Budget bindet. Hinzu kommt, dass IT-Abteilungen in KMU (falls sie überhaupt existieren) mit dem bestehenden Tagesgeschäft so ausgelastet sind, dass die Dokumentation schlichtweg hinten runterfällt. Dabei werden folgende Faktoren häufig nicht bedacht:

- IT-Dokumentation spart mittelfristig Zeit, da Anpassungen oder Netzausfälle zielgerichteter behandelt werden können und die Einarbeitung neuer Mitarbeiter einfacher umgesetzt werden kann.
- Dokumente für die Wiederherstellung der IT-Systeme sind besonders in einem Notfall relevant, um die IT-Systeme so schnell wie möglich in den Ursprungszustand bringen zu können. Daher hängt bei einer Notsituation die Handlungsfähigkeit eines Unternehmens in hohem Maße von Qualität, Aktualität und Verfügbarkeit der IT-Notfalldokumentation ab.
- Es gibt gesetzliche Vorgaben, die eine Dokumentation fordern. Dies betrifft insbesondere eine Notfalldokumentation. Aber auch IT-Sicherheitskonzepte und der Datenschutz sind relevante Bereiche.

Es hat daher für jedes Unternehmen – unabhängig von den gesetzlichen Vorschriften – Vorteile, wenn sich die IT-Dokumentation auf dem neuesten Stand befindet. Zudem sind bereits im Handelsgesetzbuch Ansätze beschrieben, die eine Verfahrungsdokumentation enthalten. Aber auch die Abgabenordnung enthält Forderungen, die in Richtung einer nachvollziehbaren Dokumentation der Geschäftsvorfälle und -abläufe gehen.

Bei den gesetzlichen Verpflichtungen stehen vor allem die Nachvollziehbarkeit und der Datenschutz im Vordergrund. Zusätzlich gewinnt im Rahmen der zunehmenden Digitalisierung die IT-Sicherheit immer mehr an Bedeutung. Auch hier sieht der Gesetzgeber die IT-Verantwortlichen zunehmend in der Pflicht und fordert diverse Maßnahmen zur Datensicherheit, die auch dokumentiert werden müssen.

Speziell die Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme gehen jedes Unternehmen etwas an und besagen, dass eine Verfahrensdokumentation aus Inhalt, Aufbau und Ablauf des Abrechnungsverfahrens vollständig ersichtlich sein muss. Für bilanzierende Unternehmen ist zusätzlich eine Bestandsdokumentation zu führen, die für Hard- und Software ein Anlagenverzeichnis vorsieht. Ein Inventarisierungs-Tool würde dabei helfen und könnte integraler Bestandteil eines Monitorings sein.

Auch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich ist mit einzubeziehen. Hier verpflich-

tet sich die Geschäftsführung, ein System zur frühzeitigen Erkennung von Bedrohungen und Risiken zu implementieren, was auch die IT-Sicherheit mittelbar betrifft. Ein Monitoring-System ist damit eigentlich vorgeschrieben, das eventuell später aufgrund steigender Sicherheitsalarme zu einem SIEM-System erweitert werden kann. Finanzdienstleister haben zudem die Mindestanforderungen an das Risikomanagement zu erfüllen, dessen Richtlinie in Bezug auf IT-Organisationen ausdrücklich ein Notfallhandbuch, das Geschäftsfortführungs- und Wiederanlaufpläne enthält, umfasst.
Zunehmende Sicherheitsvorfälle verstärken die Forderungen nach Implementierung und Zertifizierung auf Basis von IT-Grundschutz. Hier steht meistens die ISO 27001 im Vordergrund, die die Grundlage der Prüfungen des BSI darstellt. Dies gilt auch für Jahresabschlussprüfungen und Audits der internen Revision, bei denen die IT-Sicherheit immer wieder infrage gestellt werden sollte. Dabei fordert das BSI nur im Umfeld des Notfallmanagements bereits folgende Dokumentationen ein:

- Leitlinie zum Notfallmanagement;
- Bericht der Business-Impact-Analyse;
- Bericht der Risikoanalyse;
- Notfallvorsorgekonzept;
- Notfallhandbuch einschließlich Geschäftsfortführungspläne;
- Melde- und Eskalationswege;
- Übungskonzept, -pläne und -anlagen.

Im Vordergrund steht dabei der störungsfreie Betrieb, der die Verfügbarkeit auf einem höchstmöglichen Niveau halten soll. Die IT-Sicherheit ist an dieser Stelle natürlich ebenso wichtig, da sichergestellt werden muss, dass die Daten nicht nur vorhanden, sondern auch unverfälscht genutzt werden können.

Einfache Handhabung

Um die notwendige Dokumentation auf dem aktuellen Stand zu halten, ist aber auch die Handhabung, d.h. die Einbringung neuer IT-Systeme in das Monitoring, entscheidend. So ist bei Nagios und Icinga durchaus relativ viel Handarbeit notwendig, um die Systeme auf dem Laufenden zu halten. Dies kann entsprechend abschrecken bzw. hinderlich sein, so dass man in ähnliche Probleme wie bei der früheren Papiervariante läuft. Die Monitoring-Systeme InterMapper und Check_MK ermöglichen hingegen ein automatisches Erkennen aktiver Komponenten bzw. von Diensten.

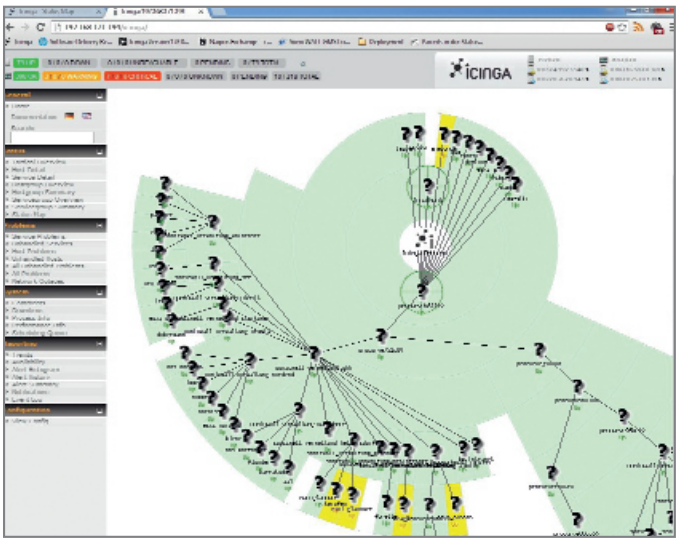

Bild 2: Topologiedarstellung unter Icinga in der klassischen Ansicht

Während InterMapper automatisiert eine Karte der erkennbaren Komponenten anlegt, die allerdings noch manuell angepasst werden sollte, geht Check_MK einen Schritt weiter. Überwachte Dateisysteme, Netz-Ports, Prozesse, Datenbanken, Festplatten usw. werden automatisch auf einem zu überwachenden Host gefunden und in das Monitoring mit aufgenommen. Dadurch verbessert sich die Handhabung erheblich und erleichtert die Arbeit des Administrators. Eine regelbasierte, hierarchische Konfiguration ermöglicht es zudem, eine entsprechende Ordnerstruktur zu verwalten, die alle Richtlinien übersichtlich hält. Auch eine Hard- und Softwareinventarisierung ist mit enthalten, so dass die Host-Informationen, die der Agent sammelt, strukturiert über eine GUI zur Verfügung gestellt oder an Drittsysteme über Datenexport weitergereicht werden können.
Check_MK wird jedes Jahr stark weiterentwickelt und hat die frühere Basis Nagios oder Icinga inzwischen weit hinter sich gelassen. Die Überwachung eines Servers greift in vielen Fällen auf einen Agent zu, der im Vorfeld auf dem Server installiert worden ist. In der Agent Bakery im Check_ MK-Host können Einstellungen und Erweiterungen der Agents zentral verwaltet und erstellt werden. Auch selbst geschriebene Dateien, sog. Custom Files, können so auf die Agents ausgerollt werden. Insbesondere in größeren Umgebungen werden die Agents-Pflege und damit die Überwachung des Servers wesentlich komfortabler. Auch die Visualisierung von Messdaten in Graphen wurde verbessert. Es ist nun möglich, beliebige Metriken, auch hostübergreifend, in einem Graphen zusammenzufassen. Diese können sowohl addiert als auch parallel oder gespiegelt dargestellt werden. Innerhalb eines solchen Graphen kann mit einzelnen Werten gerechnet werden, wodurch sich eine umfassende Auswertemöglichkeit ergibt. Neben der Erstellung von freien Graphen kann man auch vorhandene Graphen kombinieren und so vergleichen. Eine Übersichtsseite für verschiedene Graphen eines Hosts verschafft dem Nutzer einen schnellen Überblick. Die Handhabung und Visualisierung stehen damit klar im Vordergrund.

Fazit

Netzvisualisierung bei Monitoring-Systemen hilft, sich einen guten Überblick über die vorhandene Netzinfrastruktur und deren Dienste zu verschaffen. Dadurch lässt sich schneller als gewöhnlich auf Störungen reagieren. Zudem können gesetzliche Anforderungen an die Dokumentation gleich mit erfüllt werden. Ein Monitoring-System ist daher heute für jedes Unternehmen unabdingbar. Spätere Erweiterungen hinsichtlich SIEM oder Inventarisierung sind dabei ebenfalls machbar bzw. eventuell bereits enthalten, wenn die richtige Auswahl getroffen wird. *(bk)*