Für den Fall der Fälle

Die besten Sicherheitsmassnahmen nützen nichts, wenn man nicht oder zu spät erfährt, dass etwas schief läuft. Doch das Monitoring der eigenen IT ist kein Pappenstiel.

Von Richard Huber

Weiss Ihr Kunde heute vor Ihnen, dass irgendetwas nicht mehr so ist, wie es sein sollte? Erkennen Sie Netzwerkprobleme erst dann, wenn sich Benutzer beschweren? Gibt es bei Ihnen so viele Events und Alarme, dass diese prinzipiell ignoriert werden? Ist Ihre heutige Monitoring-Software zu teuer und viel zu kompliziert? Besteht Ihr Monitoring aus einer grossen Ansammlung von Skripten? Möchten Sie durch Prävention und Früherkennung Ressourcenengpässen vorbeugen?

Falls Sie eine oder mehrere dieser Fragen mit «Ja» beantworten können, sollten Sie weiter lesen. Können Sie zu jedem dieser Punkte sagen, dass das bei Ihnen kein Thema ist, dürfen Sie sich glücklich schätzen, denn dann gehören Sie zu einer Minderheit, die immer und jederzeit über den Gesundheitszustand ihrer Informatik Bescheid weiss, nicht zu viel Geld dafür ausgibt oder ganz einfach bis heute noch relativ unabhängig vom Informatikeinsatz ist.

Die verschiedenen Monitoring-Disziplinen

Doch wie kann ich sicherstellen und kontrollieren, wie «gut» es meiner IT-Infrastruktur geht, auch wenn ich nicht gerade davor stehe? Dazu zuerst ein kleiner Exkurs, welche Arten von Monitoring es überhaupt gibt:

Das **Infrastruktur-Monitoring** umfasst die Überwachung der Rechenzentrumsinfrastruktur. Dazu gehören die Stromversorgungen (z.B. USV-Anlagen), das Klima (z.B. die Klimaanlagen, Temperaturfühler) sowie die Sicherheit (z.B. Brandmeldezentralen, Gebäudeleittechniksysteme, Videoüberwachungen und Einbruchmeldeanlagen).

Das **Netzwerk-Monitoring** umfasst die Überwachung des Netzwerkes. Überwacht werden hierbei sowohl die einzelnen Komponenten (z.B. Switches, Routers, Gateways, Modems, Firewalls etc.) als auch die Verbindungen untereinander jeweils auf Verfügbarkeit und Auslastung.

Das **Server-Monitoring** überwacht systemkritische Ressourcen (CPU, Memory, Diskplatz etc.), Applikationen (Prozesse, Log Auswertungen etc.) sowie bei physischen Servern auch das Blech (Netzwerkkarten, Stromversorgung, Ventilator etc.).

Das **Service Level Monitoring** dient der objektiven Beurteilung der internen IT-Dienstleistungen, zur Optimierung der Kosten und der Steigerung der Produktivität. Service Level Agreements (SLAs) können nur durch richtiges Messen auch objektiv beurteilt werden.

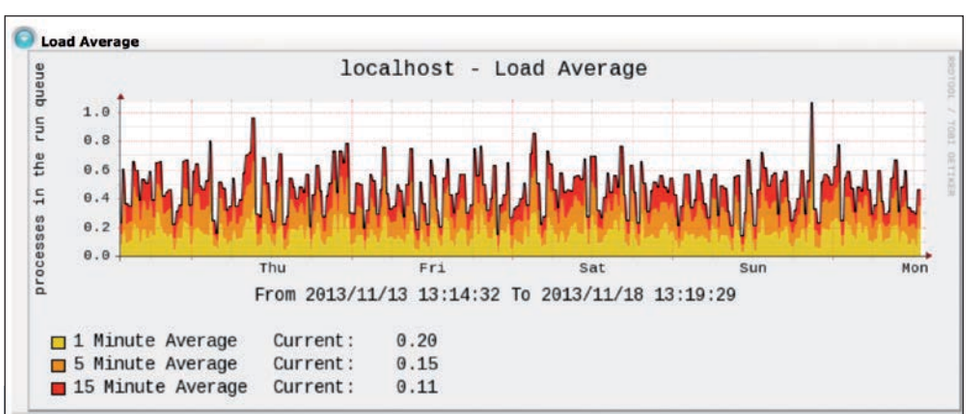
Das **Business Service Monitoring** dient zur Beurteilung der Qualität von Geschäftsprozessen. Die Abhängigkeit der Geschäftsprozesse von einer einwandfrei funktionieren IT-Infrastruktur nimmt stetig zu. Entsprechend schwierig wird es, eine 100-prozentige Zuordnung einzelner Systemzustände zu einem Business Service herzustellen.

Das **End-to-End Monitoring**, oder oft auch als User Experience bezeichnet, ermöglicht durch Simulation das Überwachen aus Sicht des Kunden. Da die Abbildung oder Korrelation des Business Service immer komplexer wird, gewinnt die echte Kundensicht betreffend Verfügbarkeit und Performance immer mehr an Bedeutung.

Weniger ist oft mehr

Der Fokus dieses Fachartikels liegt, mit Blick auf das Schwerpunktthema «Physische Sicherheit auf IT-Basis», auf dem Monitoring der eigenen Server und der Überwachung der Rechenzentrumsinfrastruktur, also dem Infrastruktur- sowie dem Server-Monitoring. Wichtig ist dabei, sich vorgängig Überlegungen zu machen, was überhaupt zu überwachen ist. Was ist sinnvoll und was lässt man lieber sein? Hier gilt, weniger ist oft mehr.

Das Zauberwort heisst also bedürfnisgerechtes Monitoring. Damit verhilft man dem Monitoring nämlich auch zur notwendigen Akzeptanz, denn es gibt nichts Schlimmeres als Fehlalarme. Fehlalarme sind Gift für jede Monitoring-Lösung und dienlichst zu vermeiden. Somit ist auch sicherzustellen, dass das Monitoring-System aktiv gepflegt wird. Änderungen in der Infrastruktur- und Serverlandschaft sind immer zeitnah nachzuführen. Es ist ein Konzept zu erstellen mit den Inhalten, was soll überwacht werden, wer ist zu alarmieren und wie sieht die Alarmierung in Abhängigkeit der Zeit aus.



Performance-Messung: Systemauslastung eines Linux-Servers.

Ein Dashboard zeigt den Gesundheitszustand der Informatik auf einen Blick.

Welche Lösung ist die richtige?

Wie erwähnt kann sehr viel gemessen und überwacht werden, von Messfühlern, Zutrittskontrollen, der USV-Anlage über den Zustand und die Auslastung der Server, CPU, Memory und Speicherplatz bis zur Verfügbarkeit der eigenen Server und Netzwerkkomponenten. Die Frage stellt sich nur, welche Mittel, welche Tools am besten dazu geeignet sind. Neben den klassischen, teuren und komplexen Tools der grossen Hersteller HP, BMC, IBM und CA, stellt sich die Frage, was der Markt heute in dieser Richtung sonst noch zu bieten hat.

In den letzten Jahren hat sich sehr viel getan und die Open Source Community hat sehr starke Tools und Lösungen hervorgebracht. Diese haben sich am Markt etabliert und die Lösungen der grossen Vier im Infrastruktur- und Server-Monitoring mehrheitlich verdrängt. Nagios gilt heute als Open Source de-facto Standard im Monitoring. Nagios besitzt eine weltweite und sehr aktive Community, die eine gewaltige Menge an Plugins hervorgebracht hat. Plugins sind Programme die Nagios zur Abfrage von Komponenten nutzt. Es gibt praktisch nichts, was mit solchen Plugins nicht abgefragt und überwacht werden könnte.

Nagios ist aber nur der eigentliche Monitoring-Kern. Nebst einer nicht sehr kundenfreundlichen Konfiguration fehlen auch weitere wichtige Komponenten wie die grafische Darstellung von Performance-Aufzeichnungen. Aus diesem Grund haben sich diverse Firmen darauf spezialisiert, um den Nagios-Kern herum ein kundenfreundliches und umfassendes Framework zu entwickeln. Dieses Framework deckt alle Monitoring-Bedürfnisse bis hin zum Service Level Management und dem Business Service Monitoring ab. Open-Source-basierende Monitoring-Frameworks sind darum heute für das Infrastruktur- und Server-Monitoring die erste Wahl.

Selber unterhalten oder auslagern

So weit, so gut. Doch wer betreibt die Monitoring-Lösung am besten? Auch hier gibt es, wie nicht anders zu erwarten, mehrere Möglichkeiten, wobei die Grösse der eigenen Informatik und das vorhandene Know-how schlussendlich die richtige Wahl, um ein qualitativ hochstehendes Monitoring zu unterhalten, massgeblich beeinflussen. Grob können drei Tendenzen unterschieden werden:

a) Betrieb und Konfiguration der eigenen Monitoring-Infrastruktur durch eigenes IT-Personal.
b) Betrieb und Konfiguration der eigenen Monitoring-Infrastruktur durch einen externen Dienstleister im Outtasking.
c) Betrieb und Konfiguration der nicht eigenen Monitoring-Infrastruktur durch einen externen Dienstleister im Outsourcing.

Es ist schwierig nur anhand des Kriteriums Unternehmensgrösse die richtige Wahl für den Monitoring-Betrieb zu wählen. Es gibt kleine Unternehmen mit einem grossen Informatikmittelbedarf und es gibt mittlere Unternehmen, die mit wenig Informatikmitteln auskommen. Es braucht also einen anderen Entscheidungsfaktor. Die Anzahl der zu überwachenden Komponenten ist ein geeigneter Indikator, wobei die nachfolgende Empfehlung als Richtlinie zu verstehen ist und von Fall zu Fall abweichen kann.

Bei weniger als 20 Komponenten ist sicher das Outsourcing ein Thema. In der Regel fehlen die personellen Ressourcen um ein gutes Monitoring zu betreiben. Eventuell wäre hier sogar ein komplettes Outsourcing aller Informatikmittel in ein externes Rechenzentrum zu prüfen. Das Monitoring könnte dann vom Rechenzentrumsbetreiber als Dienstleistung bezogen werden.

Bei 50 bis 200 zu überwachenden Komponenten ist ein Outtasking des Monitoring-Betriebes in Betracht zu ziehen. Eine Informatik mit dieser Anzahl Devices wird früher oder später mehr als nur Infrastruktur- und Server-Monitoring nutzen wollen. Dadurch wird die Komplexität aber rasch zunehmen. Möchte man das Know-how trotzdem selber im Hause behalten, sollte bei Bedarf der Rat eines Spezialisten beigezogen werden. Ebenfalls ist die Stellvertretung für den Monitoring-Betrieb nicht zu vergessen.

Bei 500 und mehr zu überwachenden Komponenten sollte der Betrieb der Monitoring-Infrastruktur durch eigenes Personal erste Wahl sein. Eine punktuelle Unterstützung durch Spezialisten ist sicher zu empfehlen. Für die Überwachung einer Infrastruktur dieser Grössenordnung sind in der Regel genügend eigene personelle Ressourcen vorhanden. Ziemlich sicher wird sich auch hier die Überwachung nicht nur auf das Infrastruktur- und Server-Monitoring beschränken.

Die Art und Weise des Monitoring-Betriebes ist sorgfältig abzustimmen. Grösse, Komplexität, eigene personelle Ressourcen und vorhandenes Know-how beeinflussen die Wahl. Nicht zu vernachlässigen: Auch ein schlecht gewartetes Monitoring bindet kostbare Ressourcen.

REMOTE-MANAGEMENT

Ergänzend zum Infrastruktur- und Server-Monitoring noch ein kleiner Abstecher ins Remote-Management. BYOD (Bring Your Own Device) ist heutzutage überall ein Thema. NYOD (Not Your Own Device) ist aber, insbesondere für das Remote-Management, ebenso wichtig. Wie erhalte ich von überall her einen hochsicheren Zugang zur eigenen Informatikinfrastruktur ohne dauernd den Firmen-Laptop dabei zu haben? Der Markt bietet dazu heute bereits einige hervorragende Lösungen basierend auf Boot- oder Office-Sticks an, die eine 100-prozentige Trennung von privater und beruflicher Nutzung garantieren.

Nehmen wir an, man sitzt bei Freunden zum Abendessen, das Monitoring funktioniert wie es sollte und vermeldet, dass der Webserver für den Online-Bestelldienst nicht mehr funktioniert. Man weiss, es ist kein Fehlalarm und es besteht Handlungsbedarf. Mit einer entsprechenden Remote-Access-Lösung man sich nun von jedem Windows-Rechner oder Mac ohne Softwareinstallationen und ohne Spuren auf dem Gastgeber-PC zu hinterlassen in die eigene Infrastruktur einloggen und den Fehler beheben. Der wichtige Online-Bestelldienst funktioniert wieder und das feine Nachtessen kann genossen werden.

Ein flexibler und doch hochsicherer Remote Access zur eigenen Informatikinfrastruktur kann also sehr hilfreich sein und ist eine ideale Ergänzung für jede Monitoring-Lösung.

Die Cloud und ihr Einfluss auf das Monitoring

Mit dem Cloud Computing kommt eine weitere Betrachtungsweise des Monitorings hinzu. Es ist zwischen Public oder Private Cloud zu unterscheiden. Private Clouds sind Umgebungen, die auf ESX, Hyper-V, Xenapp etc. basieren. Blendet man in einer vereinfachten Betrachtung die Dynamik der Virtualisierung aus, so unterscheidet sich die Überwachung hier nicht stark vom klassischen Server-Monitoring.

Natürlich gibt es auch Möglichkeiten für das Monitoring von Computerressourcen, die bei externen Providern wie Amazon, Google oder aus der Schweiz (Interoute, Green.ch etc.) bezogen werden, die also aus der Public Cloud kommen. Und die Public Cloud Provider bieten in der Regel auch eine eigene Monitoring-Dienstleistung an.

In der Praxis kommt oft der Hybrid- Ansatz zum Einsatz, also ein Teil der Informatik wird intern bereitgestellt und ein Teil der Dienste wird aus der Public Cloud bezogen. Entsprechend ist somit auch das Monitoring zu konzipieren.

Kostenlos ist nicht unbedingt am besten

Last but not least geht es immer auch um die Kosten. Doch was kostet das Infrastruktur- und Server-Monitoring? Reine Open-Source-Lösungen mit Support aus der Community sind ohne Lizenzen oder Subscriptions erhältlich. Kosten fallen einzig beim Aufbau, bei der Implementierung und vor allem bei der Pflege an.

Auf den ersten Blick scheint dies eine kostengünstige Variante zu sein. Aber Achtung: Viele Leistungen und somit verbundene Kosten werden nicht transparent ausgewiesen. Open Source basierende Frameworks bieten derweil eine viel einfachere Handhabung, eine umfassendere Lösung, Support von einem Hersteller sowie eine garantierte Produktweiterentwicklung und Innovation an. Diese Leistungen werden über Lizenzen oder Subscriptions abgegolten.

Der Kostenvergleich zwischen «Selbstbau mit Community-Support» und den kommerziellen Open-Source-Framework-Lösungen fällt darum eindeutig zu Gunsten der Frameworks aus. Sie sind bei einer ganzheitlichen Betrachtung schlussendlich günstiger.

Grosse Herausforderung Business Services

Soweit der Ausblick über die Möglichkeiten des Infrastruktur- und Server-Monitorings. Die grosse Herausforderung liegt jedoch je länger desto mehr bei der Überwachung der Business Services und bei Themen wie Event-Korrelationen, Modellierung und dem End-to-End Monitoring. Aber auch hier gilt wie überall im Monitoring «keep it small and simple», vermeide Fehlalarme, denn nur so erhält man eine hohe Qualität und ein zuverlässiges Monitoring, das ernst genommen wird.

Richard Huber ist Geschäftsführer von Realstuff Informatik. Das Unternehmen beschäftigt sich seit 2003 mit Monitoring.