



Bildquelle: Fotolia

Wer misst, misst Mist

Was in verschiedensten Firmenzweigen bereits als Arbeitsmittel zur Verfügung steht, wird je länger desto mehr auch von der IT gefordert. Dashboards, Statistiken und Auswertungen stehen heute ganz oben auf der Wunschliste der IT-Kundschaft. Wer in der Datenflut die relevanten Informationen finden will, muss verschiedene Aspekte beachten. Kaspar Geiser



Kaspar Geiser

ist Geschäftsführer und
Mitinhaber der Aspectra AG.
kaspar.geiser@aspectra.ch

IT ist heute aus keinem Geschäftsbereich mehr wegzu-denken. Dementsprechend vielseitig sind die an der IT beteiligten Personenkreise. Management und Auftraggeber fordern einfache und zum vereinbarten SLA bezogene Auswertungen. Diese sollten ansprechend präsentiert, verständlich und für die Anwender schnell abrufbar sein. Einzelne Businessabteilungen wiederum sind an spezifischen Auswertungen wie Anzahl Transaktionen, Umsatz eines Webportals oder Besucher einer Internetseite interessiert. Weitere Beteiligte sind der technischen Gruppe zuzuordnen.

Als Erstes sind hier die Applikationsentwickler zu nennen. Diese sind meistens erst beim Auftreten von Problemen einer Anwendung an Messwerten interessiert. Die Entwickler interessieren sich dann vor allem für Antwortzeiten, Prozessorauslastungen, Datenbankkapazitäten etc. Diese Daten müssen sowohl vom aktuellen Zeitpunkt als auch aus der Vergangenheit zur Verfügung stehen. Die nächste Gruppe sind die Betreiber der Server und IT-Infrastruktur. Ihr Interesse liegt in der Messung von Temperaturen, Hardwarekomponenten, der Auswertung von Back-ups, der Auslastung von Netzwerkverbindungen etc. Diese Vielzahl

von Beteiligten stellen hohe Anforderungen an die einzelnen Messungen und Präsentationen derselben.

Aktive Überwachung

Grundsätzlich können Messungen aktiv oder passiv vorgenommen werden. Mit der aktiven Überwachung wird mittels Software und in regelmässigen Zeitabständen eine Anfrage an ein System oder eine Applikation gerichtet. Das Resultat dieser Messung wird dann im Überwachungswerkzeug mit der Zeitangabe abgespeichert. Beispiel einer aktiven Messung ist die Abfrage einer Internetseite und Prüfung des Inhalts auf ein bestimmtes Wort. Mit der aktiven Messung kann ein Fehlverhalten eines Systems oder einer Anwendung festgestellt werden, bevor dies unter Umständen von den Benutzern bemerkt wird. Aufgrund dieser Messungen kann zum Beispiel das IT-Betriebsteam alarmiert werden.

Passive Überwachung

Die passive Überwachung basiert auf Logdateien. Diese stehen der Überwachung in Form von Datenbanken oder einzelnen Dateien zur Verfügung. Mittels Analysesoftware oder eigens definierten Abfragen werden in diesen Daten einzelne Merkmale oder Muster gesucht. Beispiel für eine solche Analyse ist die Suche in Firewall-Logdateien nach unerlaubten Zugriffen auf ein System. Mit der passiven Überwachung können aber auch Anomalien im Verhalten von Benutzern festgestellt werden. Sind zum Beispiel die Anzahl fehlerhafter Anmeldungen an ein System über die letzten Stunden höher als im entsprechenden Zeitabschnitt des Vortags, kann ein sicherheitsrelevanter Vorfall vorliegen. Ein solcher Zwischenfall wird dann beispielsweise an das IT-Sicherheitsteam rapportiert.

Und was kommt nach der Messung?

Mit der Messung allein werden die oben erwähnten Ansprüche keinesfalls erfüllt. Als Erstes müssen die Messresultate zentralisiert und gespeichert werden. Dies stellt unter Umständen eine technische Hürde dar, da nicht alle für eine Messung involvierten Systeme am selben Ort, geschweige denn in den gleichen Sicherheits- beziehungsweise Netzwerkzonen angesiedelt sind. Als nächster – und mit Vorteil von der Messung unabhängiger – Schritt, muss nun der gemessene Wert auf seine Integrität geprüft werden. Meldet zum Beispiel ein Temperatursensor eines Servers einen Wert von 1450 Grad Celsius, so ist entweder der Sensor defekt oder aber die Messung falsch. Ist ein Messwert gültig, muss dieser nun auf eine mögliche Über- oder Unterschreitung des für diese Messung vordefinierten Schwellenwerts geprüft werden. Meldet zum Beispiel ein Dateisystem eine Auslastung von über 80 Prozent, ist es sinnvoll, eine entsprechende Warnung zu generieren. Auf die Warnung folgt nun die Alarmierung. Bevor jedoch ein Alarm beziehungsweise eine Meldung generiert wird, müssen verschiedene Prüfungen stattfinden. Als Erstes wird

geprüft, welche Servicezeit für das entsprechende System beziehungsweise für die überwachte Komponente besteht: Muss das System nur während Bürozeiten betrieben werden, so wird im Fehlerfall morgens um 3:00 Uhr kein Alarm an die IT-Betriebsmannschaft versendet. Ebenfalls wird geprüft, wie lange ein Fehler bereits besteht und ob die definierte maximale Dauer für diesen Fehler überschritten wurde. Erst beim Überschreiten einer solchen Dauer wird ein Fehler gemeldet.

Mit der nächsten Messung wird geprüft, ob der zuvor auffällige Messwert wieder im grünen Bereich ist. Ist dies der Fall, wird wiederum anhand des vorher fest-

gelegten Verhaltens die vorangegangene Warnung gelöscht. In einem solchen Fall werden keine Meldungen generiert. Es kann jedoch auch vorkommen, dass eine Messung über mehrere Minuten oder gar Stunden einen Alarmwert anzeigt. Wird ein solcher Fehler behoben oder verschwindet von allein, ist es trotzdem sinnvoll, wenn eine Meldung über die Aufhebung des Alarms erfolgt.

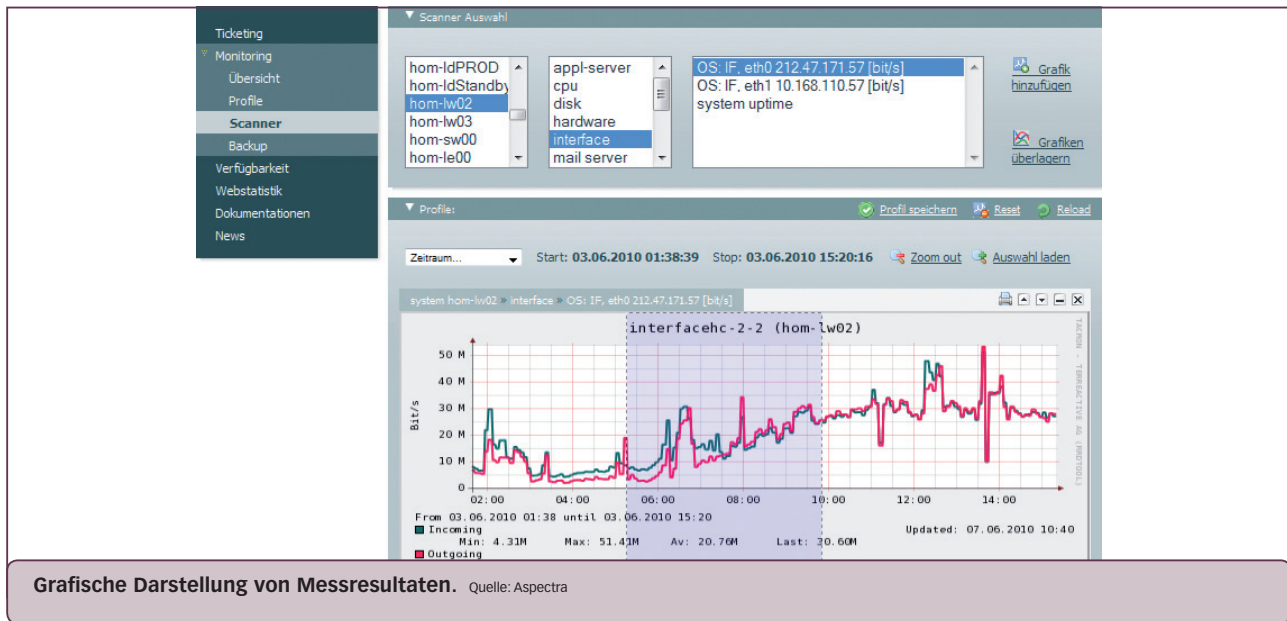
Präsentation der Messungen

Doch mit der Messung und der Reaktion auf ebendiese ist es noch nicht getan. Die nächste Herausforderung ist die Darstellung und Auffindbarkeit der Resultate. Die einfachste Präsentationsform ist der Browser, da er orts- und software-unabhängig verwendet werden kann. Die Darstellung wiederum ist von den eingangs genannten Benutzern abhängig. Es ist sinnvoll, wenn für einzelne Gruppen eigens für diese einfach verständliche Profile und Auswertungen generiert werden. Für Auftraggeber sollte zum Beispiel auf einen Blick die Verfügbarkeit einer Anwendung während der letzten zwölf Monate ersichtlich sein. Technische Mitarbeiter wiederum suchen die gewünschte Messung über Applikations- oder Systemnamen. Was die Darstellung von Messwerten betrifft, sind grafische Darstellungen am besten lesbar. Natürlich müssen den Anwendern Zoom- und Blätterfunktionen zur Verfügung gestellt werden. Auch ist es sachdienlich, wenn einzelne Perioden von Messungen, zum Beispiel eine Tages- und eine Wochenansicht einer Messung gegenübergestellt werden können, um mögliche Ausreisser einzelner Werte festzustellen. Weitere sinnvolle Unterstützungen sind vordefinierte Profile, die über mehrere Systeme einzelne Messungen zusammenfassen. So kann beispielsweise für die Kapazitätsplanung der Verlauf aller Dateisysteme über die letzten zwölf Monate angezeigt werden. Da Überwachungswerkzeuge meist für mehrere Projekte und Kunden genutzt werden, müssen die Cockpits zur Präsentation der Informationen mandatenfähig sein.

Und nach der Überwachung?

Der Einsatz von Überwachungswerkzeugen in der IT ist eine kaum mehr wegzudenkende Komponente. Doch neben der Überwachung bedarf es ebenso versiertes und erfahrenes Personal, das die gesammelten Messungen interpretieren und erklären kann. Vor allem die Spezialisten, die Systeme ▶

«Mit der Messung und der Reaktion darauf ist es nicht getan, weitere Herausforderungen liegen in der Darstellung und Auffindbarkeit der Resultate.»



und Anwendungen betreiben, müssen in der Lage sein, aufgrund verschiedener Messergebnisse die richtigen Schlüsse zu ziehen und die daraus folgenden Massnahmen einzuleiten. Eine weitere Herausforderung ist die Umsetzung der Überwachung selbst: das heisst, Überwachungsanwendungen zu realisieren, Kontrollen für die Überwachung zu definieren oder die Überwachung den aktuellen Betriebssystemen und Anwendungen anzupassen.

Lösungsansätze

Natürlich gibt es verschiedene Möglichkeiten, um eine Überwachung der IT zu realisieren. Eine mögliche Evaluation von Überwachungslösungen sollte jedoch vorsichtig durchgeführt werden. Im Markt sind sowohl Open-Source-Lösungen, komplette Lösungen der grossen Hard- und Softwarehersteller, wie auch Monitoring als Managed Service

verfügbar. Auf Open Source basierende Lösungen bedingen Know-how und Aufwand für das interne IT-Personal. Meist bieten diese Lösungen sehr viel Flexibilität in der Realisierung von eigenen Überwachungsprozeduren. Auch eignen sich Open-Source-Lösungen, wenn verschiedenste Generationen von Betriebssystemen und Anwendungen überwacht werden sollen. Komplette Lösungen der grossen Hersteller richten sich eher an homogene System- und Applikationsumgebungen. So können zum Beispiel die im Betriebssystem integrierten Überwachungsschnittstellen optimal genutzt werden. Monitoring als Managed Service zu beziehen ist dann von Vorteil, wenn keine interne Kapazitäten oder Know-how zur Verfügung stehen. Der grösste Vorteil vom Monitoring als Managed Service besteht jedoch darin, dass keine zusätzliche Hard- und Software wie auch Anbindungen an SMS/Pager-Gateways beschafft werden müssen. ■

Darstellung von aus Logdateien gewonnenen Informationen. Quelle: Aspectra

Monat	Total	OK	Error
Januar 2010	978037	973141	4896
Februar 2010	931041	926514	4527
März 2010	997393	992518	4875
April 2010	1001304	996773	4531
Mai 2010	654086	651148	2938

Monat	Total	OK	Error
Januar 2010	303	303	0
Februar 2010	255	255	0
März 2010	247	247	0
April 2010	369	369	0
Mai 2010	185	185	0

Monat	Total	OK	Error
Januar 2010	166	166	0
Februar 2010	176	171	5