



# Das Herz des Hosters: Monitoring, Alarming, Ticketing und mehr

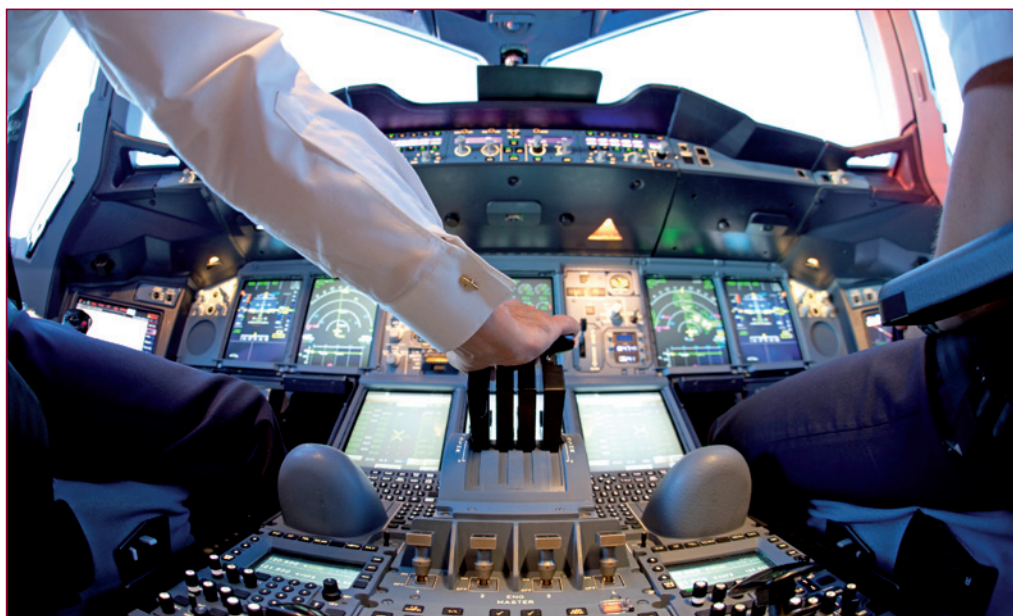
Auch in der IT werden vermehrt Dashboards, Statistiken und Auswertungen eingesetzt und stehen nicht nur ganz oben auf der Wunschliste der IT-Kundschaft, sondern sind vielmehr das Herz eines jeden Hosters und einer jeden IT-Abteilung. Kaspar Geiser

IT ist heute aus beinahe keinem Geschäftsbereich mehr wegzudenken. 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 Interessierte sind der technischen Gruppe zuzuordnen. Als Erstes seien hier die Applikationsentwickler genannt. Diese sind meistens erst beim Auftreten von Problemen einer Anwendung an Messwerten interessiert, und zwar an Antwortzeiten, Prozessorauslastungen, Datenbankkapazitäten und so weiter. Dabei müssen sowohl aktuelle Daten wie auch solche aus der Vergangenheit zur Verfügung stehen.

Als zweite Gruppe sind die Betreiber der Server und IT-Infrastruktur zu nennen. Ihr Interesse liegt in der Messung von Temperaturen, Hardwarekomponenten, der Auswertung von Back-ups, der Auslastung von Netzwerkverbindungen oder Meldungen von Sicherheitsverletzungen. Neben der umfangreichen Überwachung werden in einem Cockpit auch Prozesse wie das Ticketing und der Informationsaustausch abgebildet sowie Zugriff auf aktuelle Dokumentationen von Systemen, zum Beispiel den installierten Releases, zur Verfügung gestellt. Durch die Zusammenfassung aller dieser Daten wird das Cockpit zum Herzstück für den IT-Betrieb.

## Grundbegriff der Überwachung I: Aktive Überwachung

Grundsätzlich können Messungen aktiv oder passiv vorgenommen werden. Mit der akti-



Durch die Zusammenfassung aller Daten wird das Cockpit zum Herzstück für den IT-Betrieb. Bildquelle: Fotolia

ven 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 durch Benutzer bemerkt wird. Aufgrund dieser Messungen kann beispielsweise das IT-Betriebsteam alarmiert werden.

## Grundbegriff der Überwachung II: Passive Überwachung

Die passive Überwachung basiert auf Logdateien. Diese stehen der Überwachung als Datenbanken oder einzelne Dateien zur Verfügung. Mittels Analysesoftware oder eigens definierten Abfragen werden in diesen Daten einzelne Merkmale oder Muster gesucht. Beispiel für solche Analysen ist die Suche in Firewall-Logdateien nach unerlaubten Zugriffen auf ein System. Mit der passiven Überwachung können aber auch Anoma-

lien im Verhalten von Benutzern festgestellt werden. Ist die Anzahl fehlerhafter Anmeldungen an ein System während der 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 erwähnten Ansprüche keinesfalls erfüllt. Als Erstes müssen die Messresultate zentralisiert und gespeichert werden. Dies stellt unter Umständen eine technische Hürde dar, da nicht alle in eine Messung involvierten Systeme am selben Ort, geschweige denn in den gleichen Sicherheitsbeziehungsweise Netzwerkzonen angesiedelt sind. Als Zweites muss nun, bestenfalls von der Messung unabhängig, der gemessene Wert auf seine Integrität geprüft werden. Meldet 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

**Kaspar Geiser** ist Geschäftsführer und Inhaber von **Aspectra AG**.

vordefinierten Schwellwerts geprüft werden. Meldet ein Dateisystem eine Auslastung von über 80 Prozent, ist es sinnvoll, eine entsprechende Warnung zu generieren.

Als Drittes folgt nun die Alarmierung. Bevor jedoch ein Alarm beziehungsweise eine Meldung generiert wird, müssen verschiedene Prüfungen durchgeführt werden. Zunächst wird getestet, welche Servicezeit für das entsprechende System oder für die über-

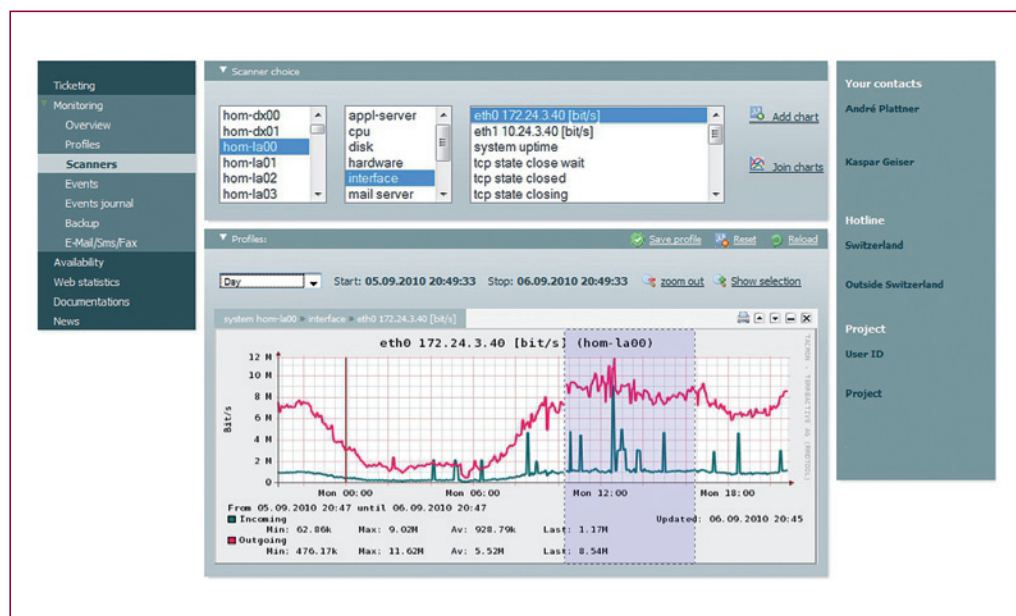
den einzelne Meldungen dem 2nd oder 3rd Level und dort jeweils einzelnen Personen zugeordnet. Natürlich bedingt die Alarmierung entsprechend hochverfügbare Systeme und Anbindungen, wie an die Pager/SMS-Provider, damit ein Alarm den entsprechenden Ingenieur auch erreicht. Daneben sind weitere Prozesse implementiert, die bei keiner Reaktion auf einen Alarm weitere Stellen alarmiert beziehungsweise an diese eskaliert.

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, sind die Cockpits zur Präsentation der Informationen mandantenfähig.

### Ticketing und mehr

Neben den reinen Messungen sowie Alarmierungen werden in einem solchen Cockpit auch Prozesse wie das Ticketing, die Informationen über anstehende Arbeiten sowie die Systemdokumentation zur Verfügung gestellt. Mit den Tickets verhält es sich gleich wie mit einer Systemmeldung mit dem Unterschied, dass auf Tickets nicht gerade innerhalb von Minuten, sondern eher von Stunden reagiert und mögliche Interventionen oder Arbeiten nicht sofort, sondern binnen beispielsweise Tagen erfolgen. Die Mechanik, also das Generieren von Warnungen oder Alarmen bei einer Nichtbehandlung durch die IT-Mannschaft innerhalb einer vordefinierten Zeit, löst wieder Alarme aus, wie wenn ein System oder eine Anwendung ausfällt.

Ähnlich, jedoch mit zum Teil menschlicher Intervention, werden Tickets mittels Workflow zudem gesteuert und weitergegeben. Mit der Anforderung vor allem aus dem Security Management kommen zudem immer mehr Funktionalitäten zur Erkennung von Sicherheitsverletzungen, wie der Veränderung einer Systemdatei, hinzu. Hierbei gilt der Grundsatz, dass Ereignisse und Dokumentationen nicht direkt von den betroffenen Systemen selbst, sondern von zentralisierten, vom eigentlich betroffenen System losgelösten Anwendungen und Datenbanken diese Informationen aufbereiten. So kann verhindert werden, dass bei einem Angriff auf ein System auch gleich die Logmechanismen oder Logdaten verändert werden. Auch werden im Cockpit Auswertungen und Statistiken von Drittsystemen entsprechend eingebunden. So wird zum Beispiel der Versand von E-Mail/Fax/SMS dargestellt. Neben den rein statistischen Informationen über erfolgreich/nicht erfolgreich und jeweils deren Anzahl dient diese Auswertung auch der Verrechnung von Dienstleistungen. Weitere, meist kompliziert in Drittsystemen verwaltete oder ausgewertete Informationen sind die Logs über Back-ups. Auch diese werden im Cockpit entsprechend verarbeitet und dargestellt und dienen neben der Information auch der Kapazitätsplanung sowie der Verteilung der verschiedenen Back-ups über die einzelnen Wochentage. <



Wenn Messdaten grafisch dargestellt werden, sind sie am besten lesbar. Bildquelle: Aspectra

wachte Komponente besteht. Muss das System nur während Bürozeiten betrieben werden, so wird im Fehlerfall morgens um 3 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 dann wird ein Fehler gemeldet. Als Viertes, beziehungsweise mit der nächsten Messung, wird geprüft, ob eine mögliche Messung wieder im grünen Bereich ist. Ist dies der Fall, wird wiederum anhand des vorher festgelegten Verhaltens die vorangegangene Warnung wieder 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 sinnvoll, wenn eine Meldung über die Aufhebung des Alarms erfolgt.

Warnungen und zum Teil auch Alarme werden aber nicht nur im reinen Incident Management verwendet, sondern können auch für das Problem- und/oder Change Management benutzt werden. Dabei wer-

### Präsentation der Messungen

Doch mit der Messung und der Reaktion auf diese ist es noch nicht getan. Die nächste Herausforderung ist die Darstellung und Auffindbarkeit der Resultate. Die einfachste, da orts- und softwareunabhängige Präsentationsform ist der Browser. Die Darstellung wiederum ist von den Benutzern abhängig. Es ist sinnvoll, wenn für einzelne Gruppen eigens für diese einfach verständliche Profile und Auswertungen bestehen. Für Auftraggeber sollte die Verfügbarkeit einer Anwendung der letzten zwölf Monate auf einen Blick ersichtlich sein. Technische Mitarbeiter wiederum suchen die gewünschte Messung über Applikations- oder Systemnamen.

Was die Darstellung von Messwerten betrifft, sind Grafiken am besten lesbar. Natürlich müssen dem Anwender Zoom- und Blätterfunktionen zur Verfügung gestellt werden. Auch ist es sachdienlich, wenn einzelne Perioden von Messungen, wie eine Tages- und eine Wochenansicht, gegenübergestellt werden können, um mögliche Ausreißer einzelner Werte festzustellen. Eine weitere sinnvolle Unterstützung sind vordefinierte Profile, die über mehrere Systeme