Intelligente Bereitstellung von IT-Services

Duales IT-Monitoring

Die Sicht auf die Verfügbarkeit der Infrastruktur reicht heute bei weitem nicht mehr aus. Verfügbarkeit und Sicherheit sollten gemeinsam betrachtet werden.

Kaum ein Unternehmen verzichtet heute auf eine kontinuierliche Überwachung seiner IT-Systeme. Bisher lag der Schwerpunkt des IT-Monitorings auf der Überwachung der IT-Infrastruktur mit dem Ziel, eingetretene oder drohende Leistungseinschränkungen und Ausfälle zu erkennen. In diesem Zusammenhang handelt es sich um das sogenannte Verfügbarkeits- und Performance-Monitoring. Die erkannten Ereignisse umfassen Defekte (etwa Hardwareausfälle), Leitungsausfälle sowie die Auslastung beziehungsweise Überlastung von Komponenten, Diensten oder Anwendungen. Das Verfügbarkeits- und Performance-Monitoring trägt somit wesentlich dazu bei, die Fehlerbehebung gezielt zu verfolgen und Ausfallzeiten beträchtlich zu minimieren. Bei redundant ausgelegten Infrastrukturen können geschäftskritische Ausfälle meist komplett vermieden werden.

Das Verfügbarkeits- beziehungsweise Performance-Monitoring verfolgt im Wesentlichen folgende Ziele:

- Überwachung der System- oder Diensteverfügbarkeit der IT-Infrastruktur
- Überwachung von Schwellwerten

Illustration: © Phatt1978/shutterstock.com

- Erfassen und Dokumentieren von Systemmeldungen
- Lieferung operativer Kennzahlen für den IT-Betrieb
- Darstellung der Auswirkungen auf die Geschäftsprozesse

Die grundsätzliche Verfügbarkeit der IT-Infrastruktur wird heute darüber hinaus mindestens genauso stark von Cyberrisiken beeinflusst, also von internen oder externen Störungen des Betriebs durch Hackerangriffe und Malware, wie etwa Verschlüsselungstrojanern. Hinzu kommen Risiken für das Unternehmen selbst. Dabei kann es sich um Erpressungsversuche, Datendiebstahl oder -verlust sowie finanzielle Schäden handeln. Des Weiteren kommt es für die betroffenen Unternehmen in der Regel zu erheblichen Reputationsschäden, wenn Dienstleistungen nicht verfügbar sind oder geschützte Informationen, insbesondere Kundendaten, veröffentlicht werden.

Aus diesen Gründen gewinnt die Überwachung auf Security-relevante Ereignisse in Form des IT-Security-Monitorings immer mehr an Bedeutung.

Der Einsatz von IT-Security-Monitoring im Überblick:

- Erkennen von Schwachstellen
- Erkennen von Anomalien und Risiken jedweder Art innerhalb der IT-Infrastruktur (Malware, Angriffe, Exfiltrationen, …)
- Überwachung identifizierter Risiken, etwa aus dem Risikokatalog des Information Security Management-Systems (ISMS)
- Lieferung von Kennzahlen zur Risikobewertung im Rahmen des ISMS

Abbildung von IT- und Business-Prozessen. Unabhängig davon, ob es sich um Verfügbarkeitseinschränkungen oder um Cyberrisiken handelt, ist es außerordentlich wichtig, schnellstmöglich die Auswirkungen solcher Ereignisse auf den Geschäftsbetrieb festzustellen. Dazu ist es notwendig, einen Überblick zu gewinnen, welche Abhängigkeiten zwischen Geschäftsprozessen, IT-Services und der darunterliegenden Infrastruktur bestehen. Nach Ermittlung der Abhängigkeiten ist es sinnvoll, diese an zentraler Stelle zu dokumentieren, vorzugsweise in einer zentralen Configuration Management Database (CMDB) beziehungsweise einer Service Management Database (SMDB). Meist erfolgt eine mehrstufige Abbildung, wobei sich in der Praxis ein vierstufiger Aufbau bewährt hat. Hier ist es zweckmäßig, auf der untersten Stufe oberhalb der Asset-Ebene mit IT-Services wie Active Directory, Datei-, Datenbank-, Druck- oder Netzwerk-Services zu beginnen. In der nächsten Stufe erfolgt die Abbildung von IT-Prozessen – ERP, Web oder Warenwirtschaft. Darauf aufbauend sollten die Geschäftsprozesse (Vertrieb, Produktion, Logistik, …) abgebildet werden (Abbildung 1).

Diese Dokumentationsdarstellung kann und sollte unverändert sowohl für das Verfügbarkeits-Monitoring als auch für das Security-Monitoring verwendet werden.

Bewertung und Kontrolle von Dienstleistern. Gerade die Sicht auf die Geschäftsprozesse ist eine sinnvolle Maßnahme, wenn die IT oder wesentliche Teile davon durch externe Dienstleister betrieben werden. Externe Dienstleister werden zwar die Infrastruktur selbst – schon im eigenen Interesse zur Sicherstellung der Einhaltung der vereinbarten SLAs – auf Fehler überwachen, Auswirkungen auf die Geschäftsprozesse des Kunden aber in den seltensten Fällen aktiv erkennen und darstellen. Noch seltener erfolgt ein umfassendes Monitoring der Cyberrisiken oder Schwachstellen. Hier ist der Auftraggeber im Rahmen des Provider-Managements gefragt, selbst oder durch einen neutralen Dritten eine entsprechende Überwachung zu etablieren, um das tatsächliche Sicherheitsrisiko abschätzen und bewerten zu können. Zudem werden Dienstleister das Thema Risikoüberwachung beziehungsweise Risikobeseitigung deutlich priorisierter und nachhaltiger angehen, wenn eine externe Kontrolle existiert. Denn im Gegensatz zur Verfügbarkeit bemerkt der Kunde bei IT-Risiken nicht unbedingt sofort, dass in seiner Infrastruktur erhebliche Gefahren für sein Unternehmen lauern.

Einheitliche Darstellung von Verfügbarkeit und Risiko. Leider existiert zum heutigen Zeitpunkt kein System, das beide Sichten – Verfügbarkeit und Risiko – in einem gemeinsamen, vollintegrierten IT-Cockpit abbildet. Gründe hierfür mögen sein, dass einerseits die marktführenden Anbieter des Verfügbarkeits-Monitorings gerade erst dabei sind, das Thema Sicherheit für sich zu entdecken. Andererseits könnte es daran liegen, dass spezialisierte Anbieter von Security-Monitoring sich vorrangig auf dieses komplexe Thema konzentrieren, um in diesem neuen und stark wachsenden Markt erfolgreich zu bestehen.

Die vier Stufen

Quelle: Controlware

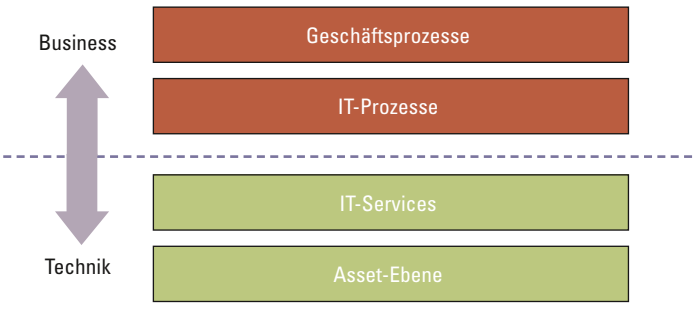

Abbildung 1: Vierstufiger Aufbau zur Abbildung von IT- und Geschäftsprozessen.

Bis solche übergreifenden Monitoring-Lösungen am Markt verfügbar sein werden, muss man entweder mit unterschiedlichen Darstellungen der jeweils verwendeten Lösungen leben (Abbildung 2) oder man setzt Tools zur Visualisierung ein, die ihren Input aus den darunterliegenden Monitoring-Systemen (Alarme und Risiken) in Verbindung mit der SMDB, in der die Geschäfts- und IT-Prozesse abgebildet sind, beziehen (Abbildung 3).

Ebenfalls zu erwarten ist, dass Monitoring-Lösungen zukünftig vermehrt in Form von modularen Managed Services angeboten werden. Dies hat den Vorteil, dass der Aufwand für den Betrieb der Lösung wegfällt. Speziell im Bereich Security-Monitoring kommt als weiterer Vorteil hinzu, dass neben dem Monitoring häufig auch die Prüfung, Bewertung und Priorisierung von Security Incidents Bestandteile von Managed Services sind. Im Gegensatz zur Bewertung von Ereignissen aus dem Infrastruktur-Monitoring stellt die Prüfung und Bewertung von Security Incidents für den Kunden eine technisch und wirtschaftlich kaum zu meisternde Herausforderung dar, müsste er dazu doch ein eigenes Security Operation Center betreiben. Kauft er IT-Security Monitoring jedoch als Managed Service ein, erhält er im optimalen Fall geprüfte, bewertete und beschriebene Incidents, die er sofort umsetzen kann. Hierbei ist allerdings darauf zu achten, geltende Datenschutzbestimmungen einzuhalten und möglichst keine kritischen Kundendaten extern, etwa in Cloud-Lösungen, zu speichern und zu verarbeiten. Controlware bietet mit seinem Customer Service Center umfangreiche Managed Services an – sowohl Infrastruktur- als auch Cyber-Security-Services.

Isolierte Sicht

Quelle: Controlware

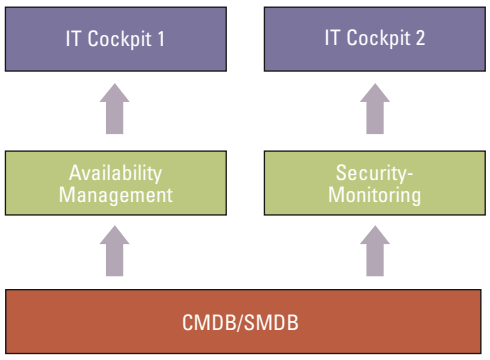

Abbildung 2: Keine gemeinsame Visualisierung.

»Leider existiert zum heutigen Zeitpunkt kein System, das beide Sichten – Verfügbarkeit und Risiko – in einem gemeinsamen, vollintegrierten IT-Cockpit abbildet. «

Eine Sicht

Quelle: Controlware

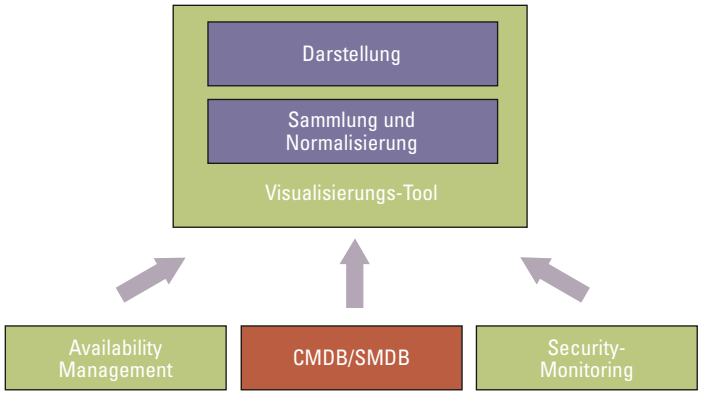

Abbildung 3: Gemeinsame Visualisierung durch zusätzliches Visualisierungs-Tool.

Fazit. Zusammenfassend lässt sich sagen, dass Verfügbarkeit und Sicherheit zwei Seiten der gleichen Medaille sind und als solche auch gemeinsam betrachtet werden sollten. Wie wir alle wissen, lassen sich technische Defekte oder Konfigurationsfehler in der IT-Infrastruktur niemals völlig ausschließen. Genauso verhält es sich mit der Sicherheit. Wir können nicht gänzlich verhindern, Ziel von Cyberattacken zu werden. Daher wäre es fahrlässig, sich nur auf die Infrastruktur-Überwachung zu konzentrieren und das Thema Cyber Security Monitoring außer Acht zu lassen. Tatsächlich ist die Frage heute nicht ob, sondern wann man von einem solchen Angriff betroffen sein wird.

Christian Bohr

Christian Bohr,
Head of Managed Services
Controlware GmbH

www.controlware.de