

Der Streit um das Service-Management

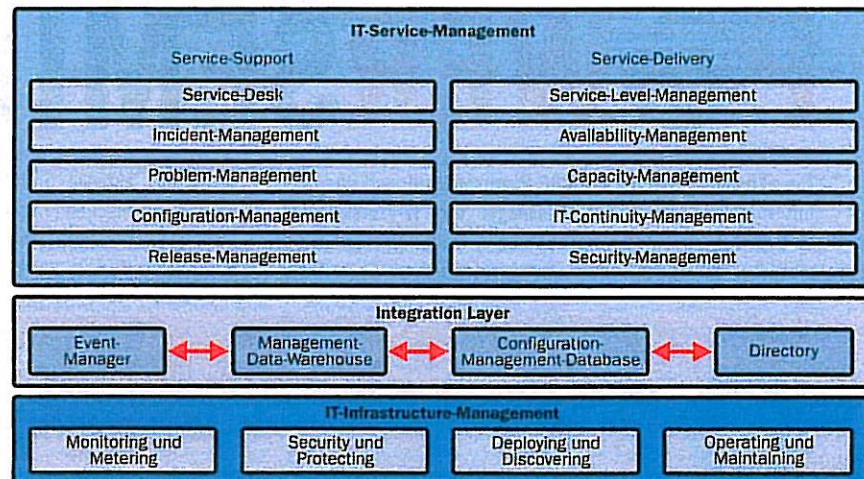
Das System-Management hat neuerdings einen kleinen Bruder zur Seite: das Service-Management. Es soll aus der IT-Abteilung einen Dienstleister machen. Doch das funktioniert nur, wenn der große Bruder mitspielt.

VON MICHAEL SANTIFALLER*

Spricht man mit den für das System-Management verantwortlichen Vertretern großer Unternehmen über ihre aktuellen Probleme, berichten sie einhellig von ihrer mangelnden Kontrolle der haus-eigenen IT-Infrastruktur. Sie wissen oft nicht, was auf ihren Servern installiert und betrieben wird, und bekommen diese Situation gegen den Widerstand von Management und Fachbereichen nicht in den Griff. Befragt man die gleichen Personen jedoch über ihre Meinung zu Itil und IT-Service-Management, kommt sofort die Gegenfrage zurück, wer denn Itil überhaupt erfolgreich einsetze.

Die andere Seite ist nicht minder verunsichert: In Workshops und einschlägigen Konferenzen verbringen Service-Management-Spezialisten viel Zeit mit

Gliederung der Administration



Quelle: Santia

Die operativen Funktionen des Infrastruktur-Managements werden mit den administrativen Aufgaben des IT-Service-Managements über einen Integration Layer verknüpft.

Hier lesen Sie ...

- ◆ weshalb sich in traditionellen IT-Organisationen zwangsläufig Konflikte zwischen System- und Service-Management ergeben;
- ◆ dass es sinnvoll ist, zunächst strikt zwischen operativen und administrativen Aufgaben zu trennen, um daraus eine Prozesskette zu schaffen, in der Mitarbeiter beide Bereiche übernehmen;
- ◆ wie dieser Workflow am Beispiel einer typischen Systemstörung aussehen kann.

Diskussionen darüber, wie strikt man vom System-Management eine Einhaltung der Change-Prozesse einfordern könne, ohne den Betrieb zu gefährden, und wie man die Zulieferung von Daten für eine Configuration Management Database (CMDB) organisieren könne. Warum funktioniert die Zusammenarbeit zwischen System- und Service-Management nicht?

Die Ursachen

Das Problem hat mehrere Ursachen auf unterschiedlichen Ebenen: der politischen, der organisatorischen und der technischen. Hier zunächst eine Analyse der organisatorischen Ebene.

Im betrieblichen Alltag sind funktionell orientierte Organisa-

tionszellen entstanden. In diesen Zellen, sie tragen in der Regel Namen wie PC-Service-, Unix-Server- oder Windows-Server-Betrieb, werden Standardprozesse zum Beispiel für die Kontrolle von Änderungen oder die Überwachung von Verfügbarkeiten und Kapazitäten reproduziert und isoliert betrieben. Management-Informationen und -Prozesse werden nicht integriert.

Hersteller orientieren sich neu

Die technische Ebene ist mit der organisatorischen eng verbunden: Die Hersteller von System-Management-Werkzeugen unterstützen durch die Entwicklung von autarken, aufgabenorientierten Produkten die prozessuale Abschottung. Dieser Trend hat sich vor einigen Jahren durch die Abkehr von Management-Frameworks und die Hinwendung zu Best-of-Breed-Produkten noch verstärkt. Allerdings beginnen die großen Management-Werkzeughersteller derzeit wieder damit, ihre Produkte stärker zu integrieren – jedoch auf einer anderen Ebene, wovon später noch die Rede sein wird.

Was also kann man unternehmen, um gleichermaßen das System-Management zu entlasten und dem Service-Management zu seinem dringend erforderlichen Einfluss zu verhelfen?

Um eine Tool-gestützte, prozessorientierte Leistungskette zu schaffen, sollte man sich zunächst vom Begriff System-Management trennen, da er im Gegensatz zum Service-Management unpräzise definiert ist und daher zu Missverständnissen führt. Besser ist es, für die operativen Aufgaben des IT-Managements den Begriff Infrastruktur-Management einzuführen. Für den Zuschnitt der Aufgaben des Infrastruktur-Managements ist es wichtig, dass es sich auf die Funktionen beschränkt, die nicht in zentraler Form vom Service-Management wahrgenommen werden. Kurz gesagt:

Infrastructure-Management ist System-Management ohne die Prozesse, die im Service-Management definiert sind.

Klare Trennung

Das Ziel dabei ist, die IT-Abteilung durch eine Anpassung der operativen Aufgaben an die zunehmende Prozessorientierung in der IT effizienter zu machen. Die Aufgabenteilung in den Prozessketten muss daher konsequent sein: Dem Service-Management kommen die überwiegend administrativen Funktionen zu, dem Infrastructure-Management die operativen. Damit wird jedoch keine bestimmte Or-

ganisation vorgegeben. Im Gegenteil: Es wird angestrebt, dass der einzelne Mitarbeiter ganze Prozessketten über die Aufgaben des Service- und Infrastructure-Managements hinweg selbstständig betreut.

Governance empfohlen

Vor diesem Hintergrund können die Leistungen des Infrastructure-Managements in vier Funktionsgruppen eingeteilt werden:

- ◆ Monitoring und Metering,
- ◆ Deploying und Discovering,
- ◆ Securing und Protecting,
- ◆ Operating und Maintaining.

Dieses funktionale Modell für das Infrastructure-Management eignet sich auch zur Abgrenzung von Leistungen, wenn auf der Plattformebene, sprich Unix- und Windows-Server, Datenbanken, Desktops etc., Betriebsaufgaben an interne oder externe Dienstleister vergeben werden. Da in der Regel die Aufgaben des Infrastructure-Managements von verschiedenen Gruppen mit verschiedenen Tools ausgeführt werden, empfiehlt es sich, eine Governance für die Infrastructure-Management-Funktionen zu etablieren, um Schnittstellen, Metriken, Leistungskriterien und Prozesse gruppen- und plattformübergreifend zu standardisieren. Auf dieser Basis können dann Operational Level Agreements (OLA) und Underpinning Contracts (UC) vereinbart werden, die jetzt auch Serviceaspekte für das Infrastructure-Management in der Zusammenarbeit mit dem Service-Management abdecken.

Vieles ist schon vorhanden

Für die technische Unterstützung von Infrastructure- und Service-Management-Prozessen ist bekanntermaßen eine Vielzahl von Tools auf dem Markt erhältlich. Um ein integriertes Service- und Infrastructure-Management zu unterstützen, muss nun analysiert werden, welche technischen Funktionen in einem Integration Layer, das heißt an der Schnittstelle zwischen den beiden Blöcken, benötigt werden.

Es fällt auf, dass hier vorwiegend altbekannte Kandidaten auftauchen, die in vielen IT-Abteilungen bereits implementiert sind oder sich in Vorbereitung befinden:

- ◆ Ein Event Manager verteilt Ereignisnachrichten aus dem Mo-

Operative Funktionen

- **Monitoring und Metering:** Überwachung von Infrastrukturelementen (Systeme, Netzwerk, Middleware, Anwendungen) sowie Erfassung von Nutzungsdaten auf diesen Elementen (Speicherplatz, Netzwerkpakete, Transaktionen usw.), typische Werkzeuge in diesem Bereich sind Monitoring-Agenten.
- **Deploying und Discovering:** Verteilung und Installation von Software und Daten, Ermitteln von Konfigurationsinformationen über Infrastrukturelemente (Inventar, Einstellungen, Beziehungen usw.). Hier werden Softwareverteilungs- und SW/HW-Inventarisierungsprodukte sowie Netzwerk-Scanner eingesetzt.
- **Securing und Protecting:** Maßnahmen und Betrieb von Anwendungen zum Schutz gegen Ausfälle und Verluste (Datensicherung), der Betriebssicherheit (Firewall, Antivirusprogramme, Spam-Filter) und der Daten (Zugriffsberechtigungen usw.)
- **Operating und Maintaining:** Operative Aktionen zur Nutzung und dem Erhalt der Betriebsbereitschaft der Infrastruktur (Storage-Management, Workload-Management, Änderungen usw.).

monitoring und Metering an Abnehmer zum Beispiel im Incident- und Problem-Management, aber auch an Abnehmer innerhalb des Infrastructure-Managements selbst, so etwa zur Versorgung von Konsolen mit Zustandsanzeigen.

◆ Eng verbunden damit ist ein Management-Data-Warehouse für die Speicherung von Management-Daten, die später unter anderem zur Problembehandlung und in fast allen Prozessen des Service Delivery ausgewertet werden.

◆ Eine Configuration Management Database ist die Basis für die Zusammenarbeit zwischen Change-, Configuration- und Release-Management sowie den Deploying- und Discovering-Funktionen. Hier wird der Soll-Zustand (deploy) dokumentiert und der Ist-Zustand (discovered) hinterlegt.

◆ Ein Directory kann die Konfiguration für Teile der Securing- und Protecting-Funktionen in Form von Benutzer- und Berechtigungsdaten liefern. In Verbindung mit der CMDB kann das Directory zum Beispiel als Grundlage für die Zuteilung von IT-Leistungen und -Berechtigungen und damit auch der Verrechnung herangezogen werden.

Der Integration Layer muss nicht nur das Service- mit dem Infrastructure-Management in-

tegrieren, sondern insbesondere auch die Daten aus den meist verschiedenen Infrastructure-Management-Tools in eine konsistente Form transformieren, damit das Service-Management mit diesen Daten arbeiten kann. Deshalb ist es unabdingbar, dass sich Infrastructure-Management-Tools mit den jeweiligen Funktionen aus dem Integration Layer integrieren lassen.

Beispielszenario

Wie passt das nun alles zusammen? Am besten lässt sich die Zusammenarbeit von Service- und Infrastructure-Management am Beispiel eines Workflows verdeutlichen, der ein einfaches, aber typisches Störungserkennungs- und Problemhebungs-szenario durchläuft.

Die Störung eines Systems, etwa der Ausfall eines Systemdienstes, wird im Monitoring durch einen Agenten erkannt und eine Nachricht (Event) über den Event-Manager an das Incident-Management weitergeleitet. Dort kommt sie als Incident-Eintrag in der Service-Desk-Software an. Der Bearbeiter stellt fest, dass die Störung bereits mehrfach aufgetreten ist und gibt den Incident als Problem weiter an das Problem-Management. Das Problem-Management zieht zur Diagnose weitere Daten über andere Systeme aus

▣ Fazit: Gewinner auf beiden Seiten

Eine bessere Integration von Service- und System-Management ist für beide Seiten und damit für das gesamte Unternehmen von Vorteil.

■ Das Service-Management gewinnt durch die Integration Zugriff auf aktuellere Management-Daten, wodurch seine Prozesse bessere Ergebnisse liefern.

■ Das System-Management erhält durch die Zusammenarbeit mehr Transparenz und Kontrolle über Konfiguration und Zustand der Infrastruktur.

■ Voraussetzung dafür ist ein neuer Zuschnitt des System-Managements in Form eines Infrastructure-Managements, um Überlappungen mit dem Service-Management auszuschließen.

dem Management-Data-Warehouse heran und entscheidet schließlich, einen Change-Request auf allen Systemen gleichen Typs vorzunehmen, um den Fehler zu beheben. In diesem Beispiel geht es darum, einen Patch für das Betriebssystem einzuspielen.

Verzweigung im Blick

Im Change-Management wird die Änderung auf ihre Machbarkeit hin geprüft. Dabei wird festgestellt, dass aus anderen Gründen bereits einige Systeme mit dem Patch versorgt wurden. Zudem erkennt man, dass es auf einem System eine Unverträglichkeit einer Anwendung mit dem geplanten Patch gibt, dieses System jedoch von dem Problem bislang nicht betroffen war. Der Change wird nun für die restli-

chen kompatiblen Systeme über einen Eintrag der geplanten Änderung in die CMDB veranlasst. Er wird an das Deployment weitergeleitet, das die Änderung vornimmt. Der neue Zustand der Systemkonfiguration wird vom Discovery gescannt und in der CMDB hinterlegt. Das Configuration-Management verifiziert im Rahmen einer Reconciliation (Abgleich) den Soll- und Istzustand und meldet dem Change-Management den Vollzug der Änderung, der Change wird geschlossen, und damit kann auch der Incident geschlossen werden.

In einem früheren, reinen System-Management-Umfeld mit isolierter Überwachung und getrenntem Patch-Management wäre das Szenario unter Umständen wesentlich ineffizienter und mit negativen Auswirkun-

gen auf den Betrieb abgelaufen. Zum einen gibt es in der Regel dort keine Protokollierung der auftretenden Fehler, und somit mangelt es an Daten über die Häufigkeit der Störungen. Das Service-Desk kennt die Ursache der Störung nicht. Folglich kann auch kein Problem-Management angewendet werden. Schlimmstenfalls wäre es dazu gekommen, dass die Störung über einen langen Zeitraum hinweg aufgetreten wäre, ohne dass eine nachhaltige Lösung für ihre Beseitigung gesucht worden wäre.

Schlecht präpariert

Irgendwann hätte man beschlossen, den Patch vorsorglich auf allen Systemen einzuspielen. Da es keine CMDB gibt, wäre es aufwändig gewesen, festzustellen, wo der Patch bereits installiert wurde. Die Unverträglichkeit mit der Anwendung hätte man nicht entdeckt, was womöglich zu Ausfällen der Anwendung geführt hätte. Insgesamt fällt bei der Betrachtung dieses zweiten Szenarios auf, dass es aufgrund fehlender integrierter Prozesse schlichtweg keine Garantie für eine effiziente und erfolgreiche Lösung des Problems gegeben hätte. (ue) ◆

*MICHAEL SANTIFALLER ist Vorstandsvorsitzender der Santix AG in Unterschleißheim bei München.