05.07.2016

SECURITY-MANAGEMENT, FACHARTIKEL

IT-Service: Bitte präventiv!

Stefan Schaffner, Geschäftsführer, ASS it-systemhaus GmbH

Wenn das Kind im Brunnen liegt, ist es buchstäblich zu spät. Im übertragenen Sinne verhält es sich so auch mit der Unternehmens-IT. Bricht beispielsweise das Netzwerk der eigenen Organisation zusammen, ist das Chaos in der Regel perfekt. Dabei lässt sich im Vorfeld nur mutmaßen, welches Ausmaß die Katastrophe annimmt. Kein Zweifel besteht allerdings darüber, dass sie negative Auswirkungen auf das Tagesgeschäft hat. Geschäftsführer und IT-Verantwortliche sind also gut beraten, wenn sie dem lieber vorbeugen. Bei der Vielzahl in Frage kommender, präventiver Leistungsangebote fällt es jedoch nicht leicht, eine Auswahl zu treffen. Denn die Verantwortlichen müssen Bedürfnisse, Chancen und Risiken gleichermaßen im Blick behalten.

IT-Organisation: Intern oder extern?

Wie relevant die Verfügbarkeit und Verlässlichkeit der IT-Systeme für ein Unternehmen ist, wissen heute kleine und mittelständische Unternehmen genauso wie die Big Player der Wirtschaft. Die Wahl eines geeigneten Monitoring- und Servicemodells muss dabei immer in Abhängigkeit des jeweiligen Organisationsmodells gefällt werden. Drei Lösungen beherrschen hier in der Regel die IT-Unternehmenslandschaften:

- Ein externer Dienstleister übernimmt vollständig die Betreuung der Informationstechnologie und Telekommunikation.
- Das Unternehmen beschäftigt eine kleine IT-Abteilung oder einen verantwortlichen Mitarbeiter als Ansprechpartner im Haus, lagert aber die Hauptleistungen an einen Dienstleister aus.
- Eine eigene, leistungsstarke IT-Abteilung kümmert sich um alle Belange und greift nur in besonderen Fällen auf Dienstleister zurück.

Die drei Ansätze eint der Versuch, die eigene IT möglichst uneingeschränkt betriebsbereit zu halten und dabei sicher aufzustellen. Dass das nicht selbstverständlich ist, fällt häufig erst im Ernstfall auf: Nämlich genau dann, wenn etwas eben nicht wie gewohnt funktioniert, Backups unbemerkt ausfallen oder ein Virus das Tagesgeschäft lahmlegt.

Prävention als Erfolgsmodell

Ist die IT erst einmal nicht mehr verfügbar, können die Fachverantwortlichen nur noch reagieren und versuchen, den Schaden zu begrenzen. Das ist weder effizient noch nachhaltig. „Aktion statt Reaktion!“ muss also die Devise lauten und „Prävention“ das Zauberwort.

Zu den zentralen, vorbeugenden Maßnahmen die IT betreffend zählt unter anderem auch die Planung einer Systemarchitektur, die in kritischen Bereichen mit Redundanzen arbeitet. Auch der Aufbau eines Kontrollmechanismus, um sich anbahnende Schäden frühzeitig zu erkennen und Gegenmaßnahmen einzuleiten, gehört zu den „Must-Haves“ einer modernen IT-Organisation. Insbesondere automatisierte 24/7-Überwachungssysteme mit definierten Handlungsvorgaben und Aufgabenzuordnungen haben sich hier in der Praxis bewährt. Damit jene ihren Nutzen voll entfalten, sollten die Handlungsfahrpläne im Störfall definiert sein und die Ansprechpartner festgelegt werden.

Daneben gilt es die Dienstleistungsvereinbarungen (SLA-Verträge) sorgsam auszuarbeiten sowie die Verfügbarkeit von Ersatz- oder Notfallsystemen sicherzustellen.

Monitoring-Systeme: Auf die Anwendung kommt es an!

Idealerweise laufen sämtliche Informationen und Daten in einem zentralen Dashboard zusammen, welches von einem Serviceteam betreut wird. Hat sich das Unternehmen für eine komplette Auslagerung der IT entschieden, bündelt ein externer Dienstleister die Daten. Dieser stößt auch die Umsetzung aller notwendigen Maßnahmen an. Bei der Kombination aus einer kleinen IT-Abteilung und externer Hauptleistung greifen beide Akteure auf die Informationen zu. Für ein effizientes Handling sind in diesem Fall die genaue Abstimmung von Handlungsreihenfolgen, -prioritäten und Zuweisungen von Verantwortlichkeiten im Vorfeld von zentraler Bedeutung.

Bei jeder Organisationsform ist eine kontinuierliche Kontrolle und Anpassung des Monitoring-Systems, vor allem hinsichtlich der Definition von Prioritäten und Risikostufen sinnvoll. Denn das beste Monitoring-Tool ist nutzlos, wenn ständige Fehlalarme oder eine Informationsüberflutung zu einer Abstumpfung der Verantwortlichen führen. Abhilfe kann an dieser Stelle die Kombination mit einem Ticketsystem schaffen, das Meldungen direkt zu Aufgaben umwandelt und sämtliche Aktivitäten dokumentiert. In Abhängigkeit von der Schwere des Vorfalls beziehungsweise der Risikostu-fe ist auch die Festlegung verschiedener Informationswege ratsam. Dazu zählen neben dem Dash-board und der Kopplung an ein Ticket-System beispielsweise die Benachrichtigung via E-Mail, SMS oder die Nutzung weiterer Benachrichtigungsdienste.

Böse Überraschungen vermeiden

Noch einen Schritt weiter als das Monitoring geht die vorbeugende Wartung und Instandhaltung von Hard- und Software, wie die ASS it-systemhaus GmbH sie mit ihren Kunden praktiziert. Ein typisches Szenario ist der präventive Austausch von kernrelevanter Hardware wie Festplatten, SSDs-, Speicher-, Akku- und Sicherungssysteme nach einem festen Wartungsplan. Denn die Wahrscheinlichkeit des Ausfalls beispielsweise einer SSD steigt mit der Betriebszeit und vor allem mit der Anzahl der Schreib-Lese-Zugriffe und ist daher vorhersagbar. Auch die Reinigung und die Durchführung von Hardware-Funktionstests in regelmäßigen Abständen zählen zu präventiven Maßnahmen, die Ausfällen maßgeblich vorbeugen. Wann was geschehen soll, sagt dem Serviceteam eine Soft-warelösung, die die Komponentengesundheit stetig überwacht.

Um schließlich nicht „Murphys Gesetz“ zum Opfer zu fallen, nach dem die Festplatte genau dann ausfällt, wenn nach fünf regelmäßig ausgeführten Präventivmaßnahmen einmal auf den Vorabtausch verzichtet wurde, sollten Unternehmen und kommunale Organisationen Wartungsverein-barungen festlegen, die auch einen Hardware-Austausch einbeziehen. Service Level Agreements sind zudem unabdingbar, um eine Unterstützung durch externe Dienstleister auch ad-hoc anfordern zu können. Dabei gehören die Definition einer schnellen Reaktionszeit genauso zu dem notwendigen Umfang wie die Vereinbarung einer mit den eigenen Risikobewertungen vereinbaren Entstörzeit sowie die Bereitstellung einer umfassenden, aktuellen Systemdokumentation.

Ausfallsicherheit durch Transparenz

Der Einsatz von Monitoring-Lösungen muss nicht teuer sein und ist mit Hilfe von modular aufgebauten Konzepten wie etwa ASSservice (in Verbindung mit ServerEye) schon für ein sehr kleines Budget und mit minimalen Betriebskosten möglich. Der Mehrwert des Einsatzes präventiver Lösungen liegt dagegen auf der Hand. Die Verantwortlichen erhalten Transparenz über ihre IT-Infrastruktur und werden durch definierbare Warnschwellen, zum Beispiel bezüglich der Speicherauslastung, Prozessorleistung (CPU) oder der Leistung des Arbeitsspeichers (RAM) frühzeitig informiert beziehungsweise alarmiert. Immer wieder gemeldete Fehlerzustände sind dabei Indikatoren für sich anbahnende Ausfälle und ermöglichen ein frühzeitiges Eingreifen. Auch die unmittelbare Benachrichtigung über den Ausfall von Hard- und Softwaresystemen oder -komponenten mit automatischer Redundanz versetzt eine Organisation in die Lage, einen sofortigen Austausch vorzunehmen um wieder redundant und damit ausfallsicher arbeiten zu können. Im Sinne der Transparenz sind auch umfangreiche Auswertungen der Monitoringwerte (Was passierte wann?), aus denen sich wichtige Informationen über die IT ableiten lassen. Auch das in den Serviceverträgen fest zu verankernde kontrollierte Patching der Betriebssysteme gegen Schwachstellen und Softwarefehler sollte lückenlos dokumentiert und archiviert werden.

Fazit

Keine Organisation kommt heute mehr ohne Informationstechnologie und EDV aus. Die Digitalisierung des Lebens und der Wirtschaft schreitet unaufhaltsam voran und hält in immer mehr Unter-nehmensbereiche und -ebenen Einzug. Schon ein Teilausfall der IT kann daher einen unternehmenskritischen Zustand bedeuten, der mit hohen Kosten und eklatanten Folgeschäden verbunden ist. Mit einem bedarfsgerechten Monitoring sind Organisationen in jeder Größe – auch

die kleineren - mit kleinen Kosten- und Zeitaufwänden geschützt und können Risiken frühzeitig erkennen und beheben. Transparenz über die Leistungsfähigkeit und Verfügbarkeit der eingesetzten Hard- und Software macht die Unternehmen und ihre Verantwortlichen handlungsfähig – ganz nach der Devise: Vorbeugen statt nachzahlen!