

Checkliste für das IT-Notfall-Management

Störungen bis hin zum Totalausfall lassen sich in der IT mit dem richtigen Notfallplan entschärfen. Folgendes sollten IT-Verantwortliche tun.

Von Markus Reitshammer, Gründer und Inhaber des IT-Systemhauses Re – Systems in Innsbruck

→ Erfassen und Analysieren der Prozesse

IT-Notfall-Management erfordert zunächst eine Business-Impact-Analyse. Dabei handelt es sich um eine Methode, die die Kernprozesse und die zugehörige Infrastruktur und IT innerhalb einer Organisation identifiziert und erfasst. So wird deutlich, welche Ressourcen den Prozessen zugrunde liegen. Die Analyse hilft auch, die Abhängigkeiten zwischen Prozessen, Services und IT-Wiederanlaufzeiten sowie die einschlägigen Schwachstellen aufzudecken.

Hierbei gilt es auch, Recovery Time Objective (RTO) und Recovery Point Objective (RPO) festzulegen: Wie lange darf es maximal dauern, bis nach einem Schaden der bewertete Geschäftsprozess voll wiederhergestellt ist? Und in welcher maximalen Zeitspanne dürfen Daten verloren gehen?

→ Notfallhandbuch erstellen

Nach der Analyse sollte ein Notfallhandbuch erstellt werden, in dem Verfahren für alle denkbaren IT-Ausfälle definiert sowie Wiederanlaufpläne erstellt und verwaltet werden. Die erarbeiteten Pläne sind ständig zu pflegen, um im Ernstfall alle Geschäftsprozesse so schnell wie möglich wieder zum Laufen zu bringen.

→ IT-Monitoring und Alerting-Systeme

IT-Monitoring- und Alerting-Systeme können beim Erstellen von Notfallhandbüchern und laufenden Dokumentationen unterstützen. Tritt ein Schaden ein, wird der zuvor hinterlegte Notfallprozess automatisch ausgelöst.

→ Notfallteams und Krisenstab

Es empfiehlt sich, ein Team zusammenzustellen, das im Notfall aktiv wird. Der Krisenstabsleiter schätzt die Auswirkungen des Notfalls ab und plant weitere Schritte.

→ Informationsfluss sicherstellen

Im Vorfeld definierte Kommunikationswege und -mittel unterstützen eine effiziente und rasche Fehlerbehebung erheblich. Dabei ist an Meldung, Eskalation und intelligente Alarmierung zu denken.

→ IT-fremde Stellen einbinden und informieren

Bei einer Störung oder einem Ausfall muss die Kommunikation mit Geschäftsführung und Abteilungsleitern funktionieren. Dazu gehören Zwischenmeldungen über den Umfang des Schadens oder die zu erwartende Ausfallzeit, aber auch Meldungen über Schadensbehebung oder Erreichen des Normalzustandes. Auf diese Weise werden Vertrauen und Stimmung im Unternehmen aufrechterhalten. Zudem dienen diese Informationen der Schadensminimierung: Betroffene Mitarbeiter können in Zeitausgleich oder Urlaub geschickt, anstehende Termine verschoben werden. Für solche Kommunikationswege gilt es ebenfalls, die Prozesse im Vorfeld zu definieren und im Alerting-Tool oder Notfallhandbuch zu hinterlegen.

→ Nichttechnische Ereignistypen

Unerwartete Störfälle von außen, beispielsweise ein Feueralarm, der Ausfall eines Outsourcers oder eine Finanzkrise, können sich kritisch auswirken. Der Umgang mit solchen Notlagen ist vorab zu bedenken.

→ Konfigurations-Reports

Eng verzahnt mit dem Notfallhandbuch sind Konfigurations-Reports. Im Gegensatz zu Leistungs- oder Verfügbarkeits-Reports werden sie für den laufenden Betrieb eingesetzt. Ein wichtiges Stichwort ist hier das „Change-Management“, in diesem Fall die kontinuierliche Dokumentation von Änderungen in der Infrastruktur.

(qua)

Fazit

Kommt es zu einem Notfall, sind diejenigen im Vorteil, die im Vorfeld die möglichen Szenarien durchgespielt, IT-Systeme, Geschäftsprozesse und Daten nach Wichtigkeit klassifiziert und die Notfalldokumentation sowie die Konfigurations-Reports laufend aktualisiert haben.