

Rechenzentren als Dienstleister

Notfallvorsorge für den Öffentlichen Dienst

(BS/Lothar Goecke*) Die IT ist fast immer eine kritische Ressource für die Erbringungen der Behördenleistungen. Der komplette und ggf. auch teilweise Ausfall eines Rechenzentrums sollte daher in das Notfallmanagement mit einbezogen werden. Ist das Rechenzentrum (RZ) nicht Teil der Behörde selbst, ist es wichtig festzulegen, wie die Verantwortlichkeiten für die Notfallplanung verteilt sind.

Die Behörde, die das Rechenzentrum nutzt, stellt Anforderungen an den Wiederanlauf der genutzten Fachanwendungen nach einem Notfall im RZ. Diese werden vertraglich für definierte Notfallszenarien, die das RZ betreffen, vereinbart. Das RZ trifft auf dieser Grundlage die dazu notwendigen technischen Vorkehrungen (z. B. Ausweich-Rechenzentrum, Auslagerung von Sicherungsmedien). Für die Zeit, bis die IT wieder zur Verfügung steht, plant die Behörde zusätzlich Verfahren für einen IT-losen Notbetrieb.

Auch bei einem Notfall innerhalb der Behörde, z. B. einem Gebäudeausfall, muss das RZ evtl. aktiv werden und Netze umschalten und/oder IKT-Komponenten in Ausweichgebäuden bereitstellen. Erforderliche RZ-Leistungen sind ebenfalls vertraglich zwischen Behörde und RZ zu vereinbaren und technisch durch das RZ umzusetzen.

Für die beiden obengenannten Fälle sind dazu noch gegenseitige Alarmierungs- und Kommunikationsverfahren zu vereinbaren.

Das Rechenzentrum selbst muss ein eigenes Notfallmanagement aufbauen. Dessen Aufgabe ist es zum einen, Anforderungen der Behörden umsetzen. Daneben plant es für die eigenen Notfälle den Wiederanlauf der Basisinfrastruktur und Geschäftsprozesse, die wiederhergestellt werden müssen, bevor mit dem Wiederanlauf von Kundenanwendungen begonnen werden kann.

Regelmäßige Tests und Übungen müssen auch hier abgehal-

ten und vertraglich vereinbart werden.

Schnittstellen zu Nachbardisziplinen

Die wichtigsten Schnittstellen des Notfallmanagements bestehen zum Krisenmanagement (KM), zum Risikomanagement (RM) und zum Informationssicherheits-Management (ISM).

• *Krisenmanagement*

Das KM steuert eine Behörde in außergewöhnlichen Situationen. Dazu zählen auch Notfälle. Nach dem Eintritt von Notfällen ist das KM die übergeordnete Institution zur Steuerung der Notfallbewältigung.

• *Risikomanagement*

Die Risikoanalysen des ISM und Notfallvorsorge gehören zum Feld der operationellen Risiken und ergänzen das allgemeine Risikomanagement der Behörde. Das allgemeine Risikomanagement betrachtet in der Regel keine einzelnen Ressourcen, sondern stellt ohne Berücksichtigung der IT-Struktur allgemeinere Betrachtungen an. Eine Absprache und Abgrenzung über Betrachtungstiefen sowie den Austausch von Kennzahlen ist dringend erforderlich.

• *Informationssicherheits-Management*

Das Notfallmanagement sichert die angemessene Verfügbarkeit und Wiederherstellung kritischer Ressourcen aller Art, die zur Ausübung kritischer Geschäftsfunktionen benötigt werden. Das ISM sichert angemessene Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit der genutzten Informationen und deren Verarbeitung. Die gemeinsame Schnittmenge ist die Verfügbarkeit von Informationen. Notfallvorsorge wird auch für Behörden mehr und mehr zu ei-

nem Thema, das systematisch behandelt werden muss. Die vorliegende Artikelserie hatte das Ziel, die wesentlichen Phasen des dazu erforderlichen Business Continuity Managements darzustellen und auf einige behörden-spezifische Fragestellungen bei der Konzeption und Planung einzugehen. Natürlich gibt es weitere Aspekte wie z. B. die Organisation, Dokumentation oder Pflege des Notfallmanagements, die hier nicht ausreichend behandelt werden konnten. Zur weiteren Vertiefung beachten Sie bitte dazu auch das Praxisseminar "Notfallvorsorge" des Behörden Spiegel am 29. & 30. September 2011 in Bonn.

Weitere Informationen und Anmeldung unter: www.fuehrungskraefte-forum.de

*Lothar Goecke ist Geschäftsführer der consequa GmbH.