K-Fall-Vorsorge für Informations- und Kommunikationstechnologie

Andreas Kernke

Infrastrukturplanung
Stadt Köln
Amt für Informationsverarbeitung
Willy-Brandt-Platz 3
50679 Köln
andreas.kernke@stadt-koeln.de

Abstract: Mit der fortschreitenden Unterstützung der Arbeitsabläufe gerade in der öffentlichen Verwaltung stieg die Technikabhängigkeit zur Erfüllung der Aufgaben. Informationen aus Aktenvorgängen, Berechnungen, Datenbankinhalten und Auswertungen sind häufig vollständig ausschließlich in digitaler Form verfügbar. Der manuellen Verarbeitung bei einem möglichen Technikausfall sind daher enge Grenzen gesetzt. Notfallplanungen für einzelne Dienste und Systeme, für Gebäude und Einrichtungen sowie für gelegentlich eintretende oder jedenfalls wahrscheinliche Szenarien sind in der Regel Gegenstand isolierter Betrachtungen. Komplexe Interdependenzen sowie iterative Ursachen- und Wirkungsammenhänge werden dabei nicht hinreichend berücksichtigt. Insbesondere unter Berücksichtigung möglicher Katastrophenfälle ist es erforderlich, diesbezügliche Einzelplanungen zu vervollständigen und einer umfassenden Gesamtbetrachtung zu unterziehen.

1 Einleitung/Notwendigkeit einer Katastrophenfall-Vorsorge

Computerunterstütztes Arbeiten hat in sehr weiten Teilen des Alltags manuelle Bearbeitung verdrängt. Routineaufgaben aber auch komplexe Planungs- und Produktionstätigkeiten können mit Technikunterstützung präziser, schneller und einfacher durchgeführt werden als ohne sie. Dadurch fanden und finden auch organisatorische Umstrukturierungen statt. Menschliche Arbeitskraft wird von einfachen Routinetätigkeiten entlastet. Gleichzeitig wird die Kompetenz, automatisierte Prozesse ohne Technikunterstützung manuell durchzuführen, abgebaut. Der Einsatz moderner Informations- und Kommunikationstechnik schafft aber auch neue Möglichkeiten kollaborativen Arbeitens. Technikunterstütze Prozesse haben sich sehr schnell und sehr umfassend etabliert. Eine Rückkehr zu den Arbeits- und Kommunikationstechniken der vergangenen Dekade wäre gar nicht mehr denkbar.

In den Anfangszeiten der automatisierten Datenverarbeitung wurden Maschinen lediglich dazu verwendet, Arbeitsergebnisse in Papierform zu produzieren, die dann in dieser Form gelagert werden konnten. Das nicht stoffliche Gut Information wurde auf einem physikalischen Träger gehandhabt, der ohne technische Hilfsmittel genutzt werden konnte. Inzwischen werden große Datenmengen ausschließlich in digitaler Form auf magnetischen oder optischen Speichermedien bereitgehalten, die ohne geeignete elektronische Systeme nicht gelesen werden können.

Behörden und Unternehmen in entwickelten Ländern befinden sich daher in einer weit reichenden Abhängigkeit von Technologie. Aktuelle technische Systeme tragen dieser Tatsache durch Redundanzen von Bauteilen und einem auf hohe Ausfallsicherheit ausgelegten Design Rechnung. Dadurch werden Systemausfälle aufgrund von technischen Störungen weitestgehend vermieden. Eine Vorsorge für den Fall größerer Schadensereignisse (Katastrophenfallvorsorge) bedarf allerdings einer umfassenderen, systematischen Betrachtung und vollständigen Dokumentation.

2 Katastrophen-/Notfallszenarien und Beeinträchtigung der IuK

Großschadensereignisse können die Verfügbarkeit von Informations- und Kommunikationstechnologie beeinträchtigen. Eine organisatorisch und wirtschaftlich zweckmäßige Konzentration von technischen Komponenten in Technikräumen und Rechenzentren führt auch zu einer Konzentration des Schädigungspotenzials. Im Folgenden werden denkbare Katastrophenszenarien beschrieben, die Auswirkungen auf die Technikverfügbarkeit haben können.

2.1 Flächendeckender Stromausfall

Ein räumlich eng begrenzter Ausfall der Stromversorgung kann zu partiellen Beeinträchtigungen führen, denen mit verhältnismäßig geringem Präventions- oder Substitutionsaufwand begegnet wird. Fällt allerdings die Stromversorgung großflächig weg, so ergeben sich daraus besondere Problemstellungen. In diesem Fall wird es erforderlich, zahlreiche Informations- und Kommunikationssysteme an mehreren Standorten mit Notstrom zu versorgen. Dies kann insbesondere bei länger anhaltenden Stromausfällen problematisch werden.

2.2 Hochwasser

Hochwasser kann auf vielfältige Art die Verfügbarkeit von Technikunterstützung beeinträchtigen. Da Elektronik naturgemäß feuchtigkeitsunverträglich ist und technische Geräte in der Regel auch nicht wasserdicht konstruiert sind, führt ein Wassereinbruch in Technikräumen zwangsläufig zu Ausfällen. Auch wenn Rechenzentrumsräume oder Räume in denen Netzwerkkomponenten installiert sind, trocken bleiben, kann dennoch die Stromversorgung beeinträchtigt sein. Auch sind Situationen denkbar, in denen Hochwasser Technikern und Anwendern den Zutritt zu Technik- und Büroräumen verwehrt.

2.3 Standortuntergang durch terroristische Anschläge/Flugzeugabsturz

Nach dem Terroranschlag auf das World Trade Center am 11. September 2001 ist eine Bedrohung Realität geworden, die bisher allenfalls theoretischer Natur war. Ein Absturz eines Flugzeuges auf ein Gebäude oder ein Sprengstoffanschlag können die darin befindliche Technik zerstören. Da ein wirksamer Schutz vor diesen Anschlägen nicht denkbar ist, kann Vorsorge hier nur aus Substitutionsstrategien bestehen.

2.4 Rechenzentrumsausfall durch Brand

Neben Wasser ist Feuer die häufigste Ursache für Computerausfälle. Ein Brand in einem Rechenzentrum oder einem direkt angrenzenden Raum kann durch Materialreaktionen von zum Beispiel Betonwänden, durch Hitze und Flammen zu Beschädigungen und Ausfällen führen. Auch Löschwasser das in Geräte eindringt, ist als Schadensursache denkbar. Brandprävention in Technikräumen und um sie herum ist daher von erheblicher Bedeutung.

3 Ausfallprävention und Substitutionsszenarien

Technische Systeme im Rechenzentrumseinsatz sind in der Regel nach dem Stand der Technik ausfallsicher konstruiert. Notwendige Komponenten sind hochredundant verbaut, um Beeinträchtigungen durch technische Defekte zu verhindern. Auch Rechenzentrums-Infrastruktur wird vorsorglich hochredundant ausgelegt. Ein noch höheres Maß an Ausfallsicherheit wird durch Redundanz der Rechenzentrumsstandorte erreicht. Dabei werden technische Systeme auf zwei oder mehr Standorte verteilt aufgebaut. Je nach technischer Architektur der eingesetzten Hard- und Software können verschiedene Verfügbarkeitsklassen realisiert werden. Eine echte Bündelung der Systeme zu so genannten Clustern mit redundanter Datenhaltung an beiden Standorten kann Ausfälle selbst bei einem Standortuntergang ganz vermeiden oder zumindest auf kurze Umschaltzeiten reduzieren. Wenn Ausfallzeiten im Bereich einiger Stunden tolerierbar sind, dann können Backup-Rechenzentren betrieben werden, in denen bedarfsweise dort bereitgehaltenen Ersatzsystemen zum Einsatz gebracht werden. Dazu müssen diese Ersatzsysteme aber laufend auf einem den Hauptsystemen äquivalenten Konfigurationsstand gehalten werden; dies stellt eine besondere Herausforderung für Konfigurations- und Veränderungsmanagement dar.

Gegen Stromausfälle werden Technikinfrastrukturen durch Notstromversorgungssysteme in Form von Dieselaggregaten und Batteriepufferungen abgesichert. Hier ist zu beachten, dass die bereitgehaltenen Kapazitäten der Fortentwicklung der Rechenzentren angepasst werden. Soweit verfügbare Kapazitäten nicht für die Aufrechterhaltung des gesamten Betriebes ausreichen, muss nach Verfügbarkeitsanforderungen priorisiert werden. Nicht alles, was in Normalsituationen zweckmäßig und nützlich ist, ist in Katastrophenfällen wirklich unverzichtbar. Hohe Priorität haben in solchen Fällen einge-

richtete Krisenstäbe, Organisationseinheiten, die an Notfalleinsätzen beteiligt sind oder die Information der Bevölkerung sicherstellen.

Neben den technischen Vorkehrungen ist die Verfügbarkeit von personellen Ressourcen insbesondere in Ausnahmesituationen sicherzustellen. Hierzu ist für Operatoren und Administratoren eine Dienstzeit- und Rufbereitschaftsregelung zu treffen. Auch die Verträge mit externen Dienstleistern und Zulieferern müssen hinsichtlich Reaktions- und Leistungszeiten betrachtet werden.

Die Hochverfügbarkeit in den Rechenzentren stellt isoliert betrachtet noch nicht die Nutzbarkeit der Technik sicher. Damit Anwenderinnen und Anwender mit einer Technikunterstützung arbeiten können, ist die Verfügbarkeit von Rechenzentrumsinfrastruktur von aktiven und passiven Netzwerkkomponenten, von System- und Anwendungssoftware, von Daten und Userendgeräten erforderlich. Daher sind alle Voraussetzungen für einen funktionierenden Einsatz von Informations- und Kommunikationstechnologie einer Gesamtbetrachtung zu unterziehen.

Redundanz von Komponenten oder Rechenzentrumsstandorten erhöht die Betriebskosten. Aus wirtschaftlichen Gründen kann es daher zweckmäßig sein, Synergien zu nutzen. Lassen sich zum Beispiel zwei Server, die für unterschiedliche Anwendungen eingesetzt werden, auf zwei Standorte verteilt clustern, so erhöht man die Verfügbarkeit ohne nennenswerte Kostenerhöhung. Dies erfordert, dass die Anwendungen untereinander verträglich sind und im Schadensfall mit den Ressourcen eines Standortes auskommen würden. Durch einen Betriebsverbund von Partnern, die jeweils ein Rechenzentrum unterhalten, können Kostenvorteile bei der Realisierung eines Zwei-Standorte-Konzepts erzielt werden. Hierzu ist jedoch eine weit reichende technische und organisatorische Anpassung beider Partner erforderlich.

4 K-Fall-Tests

Technische und organisatorische Maßnahmen zur Vermeidung oder Handhabung von Technikausfällen müssen hinsichtlich ihrer Wirksamkeit überprüft werden. Bei der Inbetriebnahme einzelner Systeme werden diese in der Regel Ausfalltests unterzogen. Diese Ausfalltests beziehen sich dabei aber auf den möglichen Ausfall von Teilen der in Betrieb zu nehmenden Systeme und nicht auf Großschadensereignisse mit weit reichenden Auswirkungen. Maßnahmen zur Prävention von Ausfällen aufgrund von Katastrophenfällen bedürfen einer umfassenden Erprobung ihrer Wirksamkeit. Dies geschieht in so genannten K-Fall-Tests. Aus Investitionsschutzgründen werden dazu natürlich keine Rechenzentren geflutet oder in Brand gesetzt. Vielmehr werden solche Katastrophenfälle simuliert. Trennt man zum Beispiel die Netzwerkverbindung zwischen zwei Rechenzentrumsstandorten so stellt sich das für beide Standorte so dar, als wenn der jeweils andere Standort untergegangen wäre. Für einen Test der Notstromeinrichtungen mag ausreichen erscheinen, die Verbindung dieser Einrichtungen mit dem Stromnetz zu unterbrechen. So lässt sich überprüfen, ob die Notstromeinrichtungen funktionieren und in vorgesehener Weise ihren Betrieb aufnehmen. Gewissheit darüber, ob auch die durch diese Notstromeinrichtungen abgesicherten Systeme bei einem Stromausfall fehlerfrei arbeiten würden,

erhält man allerdings erst durch eine echte Stromabschaltung. Dabei zeigt sich dann, ob die Versorgungskapazitäten ausreichen, eine unterbrechungs- und schwankungsfreie Stromversorgung sicherzustellen. Aufgrund unerwarteter Umstände können bei K-Fall-Tests Technikausfälle eintreten. Außerdem können Systeme, die aus wirtschaftlichen oder technischen Gründen nicht ausfallsicher ausgelegt sind, im Rahmen solcher Tests in ihrer Verfügbarkeit beeinträchtigt werden. Dies ist bei der Planung der K-Fall-Tests zu berücksichtigen. Um der Alterung und Fortentwicklung der Technikausstattung Rechnung zu tragen, müssen K-Fall-Tests regelmäßig wiederholt werden.

5 Regelmäßige Fortschreibung der Dokumentation

Technische Infrastrukturen sowie organisatorische und gesetzliche Rahmenbedingungen unterliegen einer stetigen Weiterentwicklung. Dadurch ändern sich laufend die Verfügbarkeitsanforderungen einerseits und die Ausfallsicherheiten sowie Fehlertoleranzen andererseits. Das bedingt, dass sämtliche Maßnahmen zur Vermeidung von Ausfällen sowie deren Dokumentation an veränderte Begebenheiten anzupassen sind. Soweit nicht eine kontinuierliche Fortschreibung im Rahmen jeder einzelnen Inbetriebnahme betrieben wird, sind regelmäßige Reviews durchzuführen.