Bundesamt
für Sicherheit in der
Informationstechnik

Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189, 53175 Bonn ▪ Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 ▪ Fax: +49 (0) 1888 9582-400 ▪ Internet: www.bsi.bund.de

1 Vorbemerkungen

Besonders bei Behörden oder Unternehmen mit einem umfangreichen IT-Betrieb und hohen Verfügbarkeitsanforderungen wird häufig die Nutzung eines Ausweich- oder Redundanzrechenzentrums als Maßnahme zur Notfallvorsorge in Betracht gezogen. Der Grundgedanke ist dabei, dass eines der Rechenzentren (RZ) möglichst den gesamten zentralen IT-Betrieb übernehmen kann, wenn das jeweils andere Rechenzentrum nicht voll funktionsfähig ist. Dieser Ansatz lässt sich gegebenenfalls auch auf mehr als zwei Rechenzentren verallgemeinern.

In diesem Zusammenhang wird an das Bundesamt für Sicherheit in der Informationstechnik (BSI) häufig die Frage gerichtet, welchen Abstand redundante RZ haben sollten und ob es hierzu verbindliche Regelungen oder Vorschriften gibt.

Die nachfolgenden Kapitel enthalten Hinweise und Empfehlungen zu den fachlichen Aspekten dieser Fragestellung. Diese Hinweise beruhen auf praktischen Erfahrungen und üblichen Gefährdungsszenarien. Sie sind in jedem Fall auf den jeweils vorliegenden Anwendungsfall anzupassen.

Leider kann das BSI die individuelle Vorschriftenlage, in der sich eine Institution bewegt, nicht beurteilen. Jede Institution ist deshalb in der Pflicht zu prüfen, ob für das jeweilige Vorhaben zwingende Regelungen oder Vorschriften gelten, die selbstverständlich eingehalten werden müssen und die möglicherweise von den nachfolgenden Empfehlungen abweichen.

2 Grundüberlegungen

Ausgangspunkt der Planung sind in der Regel die folgenden Zielsetzungen, die in der Praxis meist unbestritten sind:

- Beide RZ sollen nicht im gleichen Brandabschnitt eines Gebäudes liegen.
- Beide RZ sollen so angeordnet sein, dass sie möglichst nicht gleichzeitig durch das gleiche Schadensereignis betroffen sein können.
- Die Ausfallzeit, also die Zeitspanne zwischen dem Eintreten einer Störung und der Übernahme des IT-Betriebs durch das jeweils andere RZ, soll möglichst gering sein. In vielen Fällen wird sogar ein unterbrechungsfreier IT-Betrieb gefordert.

Häufig fließen weitere Anforderungen ein, die sich jedoch meist nicht verallgemeinern lassen.

Die optimale Entfernung wird durch gleichviel Sicherheitsaspekte zu großen Zahlen wie zu kleinen Zahlen getrieben:

- Je geringer der Abstand ist, desto größer ist das Risiko, dass ein Schadensereignis zugleich beide RZ beeinträchtigt.
- Je größer der Abstand ist, desto größer werden die technischen Probleme, einen Echtzeit-Parallel-Betrieb zu realisieren.

Grundsätzlich ist die Entfernung anhand einer individuellen Betrachtung aller Randbedingungen festzulegen. Dabei ist die optimale Entfernung dem Schutzbedarf und dem als realistisch angenommenen Bedrohungsszenario entsprechend zu definieren.

3 Minimalabstand

Als realistische Bedrohungsszenarien kommen in der Praxis zum Beispiel Unfälle mit Gefahrguttransporten, Großbrände, Gebäudeabrisssprengungen aber auch Bombenfunde aus dem 2. Weltkrieg in Betracht. In allen diesen Fällen muss mit einem Evakuierungs- und Sperr-Radius von bis zu 1500 m um den Schadensort herum gerechnet werden.

Unter diesen Aspekten sollte der Abstand inklusive eines Sicherheitszuschlags etwa den dreifachen Radius, also rund 5 km, nicht unterschreiten. Ist der Abstand geringer als der doppelte Radius, also kleiner als 3 km, kann es passieren, dass beide RZ innerhalb der Sperrzone liegen und somit beide nicht erreichbar sind.

Gibt es Randbedingungen, die zu sehr geringen Entfernungen zwingen, sollte mindestens eines der beiden RZ so ausgestattet sein, dass es aus der Ferne betreut und gesteuert werden kann. Damit kann zumindest für einen begrenzten Zeitraum der Betrieb aus sicherer Entfernung aufrecht erhalten werden.

4 Maximalabstand

Zu großen Entfernungen hin ergeben sich meist aus übertragungstechnischen Aspekten Grenzen. Die Probleme beginnen typischerweise ab ca. 10 bis 15 km. Hinzu kommt, dass außer massiven Kriegshandlungen kaum ein Schadensereignis realistisch angenommen werden kann, das einen so großen Bereich hinreichend stark beeinträchtigt, dass nicht mindestens eines der beiden RZ betreibbar wäre. Selbst der großflächige und mehrere Tage dauernde Stromausfall im Münsterland im November 2005 hätte hier kein besonderes Problem dargestellt, wenn zwar beide RZ betroffen, beide aber mit einer korrekten Netz-Ersatztechnik ausgerüstet gewesen wären.

Entfernungen im kleineren zweistelligen km-Bereich, also bis 50 km, dürften für die meisten Fälle ausreichend sein.

Sind die technischen Probleme lösbar oder bestehen sie auf Grund der speziellen Kommunikationsart zwischen den beiden RZ nicht, sind erheblich größere Abstände wählbar. Bei Entfernungen deutlich im zwei- oder sogar dreistelligen km-Bereich (also ab 50 km und mehr) ist jedoch ohne Kenntnis weiterer Details kein relevanter Unterschied für die Sicherheit der RZ zu sehen.

5 Spezielle Sicherheitsbetrachtungen

Ereignisse wie die Terroranschläge am 11. September 2001 in New York und Washington oder der Tsunami am 26. Dezember 2004 in Südostasien wurden, bevor sie geschahen, als "nach menschlichem Ermessen auszuschließen" betrachtet. Wenn auch solche Ereignisse berücksichtigt werden sollen, müssen sehr spezielle Sicherheitsbetrachtungen vorgenommen werden, die über den Rahmen dieser allgemeinen Empfehlung und Hinweise hinausgehen.