Hinweis zur Norm

Komiteeverlautbarung GK 719 zum BSI-Dokument „Kriterien für die Standortwahl höchstverfügbarer und georedundanter Rechenzentren“, 2018

Das BSI Dokument „Kriterien für die Standortwahl höchstverfügbarer und georedundanter Rechenzentren“, das Ende des Jahres 2018 erschienen ist, hat in der deutschen Rechenzentrumsbranche für einige Verunsicherung gesorgt. Als deutsches, nationales Gremium zur Entwicklung und Fortschreibung der Rechenzentrumsnormen DIN EN 50600 (VDE 0801-600) sowie der fachlich verwandten Dokumente aus CENELEC und ISO/IEC haben die in DKE/GK 719 „Rechenzentren“ tätigen Fachkreisvertreter das vorgenannte Dokument mit Erstaunen zur Kenntnis genommen und sehen sich aufgefordert Stellung zu nehmen.

Zusammenfassung

Das GK 719 nimmt wie folgt Stellung zum BSI-Dokument „Kriterien für die Standortwahl höchstverfügbarer und georedundanter Rechenzentren“:

- Eine Risikobetrachtung und -bewertung ist grundsätzlich einem Vorgehen mit Hilfe fester Vorgaben für Abstände vorzuziehen
- falls feste Vorgaben aus Sicht des BSI erforderlich oder sinnvoll sind, sollte eine klare, nachvollziehbare Herleitung der empfohlenen Abstände dargestellt werden
- eine stärkere Anlehnung der BSI-Dokumente an die EN 50600 unterstützt die Anwendung der relevanten Vorgaben
- eine stärkere Zusammenarbeit mit dem GK 719 unterstützt eine starke europäische und internationale Position für die Sicherheit von Rechenzentren

Im Einzelnen:

1. Zunächst wird in der Einleitung in einer Fußnote auf die Definition von Rechenzentren im Anhang 4.3 des Dokuments verwiesen. In diesem Anhang wird folgende Aussage getroffen: Zitat: *„Die RZ-Definition aus den Anfangsjahren des BSI-Grundschutzes um 1995 ist nicht mehr zeitgemäß und lässt sich auch nicht mit der DIN EN 50600 in Deckung bringen.“*
   In der anschließend beschriebenen Definition ist nicht erkennbar, in welchen Punkten es keine Deckung mit der EN 50600 gibt. In der EN 50600 wird davon ausgegangen, dass unabhängig von Größe und Zweck eines Rechenzentrums die Norm immer dann angewendet werden kann und sollte, wenn dem Rechenzentrum für den Unternehmenszweck eine entsprechende Bedeutung zukommt, so dass die verwendeten Grundsätze der Verfügbarkeit, Sicherheit und Befähigung zur Energieeffizienz sinnvoll angewendet werden können.

2. Weiterhin wird im Abschnitt 1.2 „Verfügbarkeit“ auf die vom BSI verwendeten Verfügbarkeitsklassen verwiesen, die über Zielverfügbarkeiten in % (99,99 % pro Jahr für VK 3 und 99,999 % pro Jahr für VK 4) bzw. maximale Ausfallzeiten definiert sind. Die EN 50600 definiert 4 Verfügbarkeitsklassen und verzichtet dabei bewusst auf die Nennung von Zahlen, da solche Zahlen aus Sicht des Gremiums statistischer Grundlagen entbehren und eher falsche Erwartungen befördern. Die Verfügbarkeitsklassen der EN 50600 basieren auf Designprinzipien zur Absicherung der geforderten oder gewählten Verfügbarkeit wie „Mehrpfadigkeit“ oder „Redundanz von Komponenten“. Planer, Errichter und Betreiber können so besser Risiken verstehen und ggf. Schwächen im Design oder im Betrieb gezielt betrachten und beseitigen. Weiterhin wird die reale Verfügbarkeit neben dem Design auch entscheidend von der Umsetzung von Betriebsprozessen beeinflusst.

DKE
VDE DIN

3. Der Abschnitt 1.3 „Öffnungsklausel“ enthält aus unserer Sicht Aussagen, die zu breiter Verunsicherung führen:
   I. Zitat: *„Es ist unmöglich, alle in der Realität möglichen Varianten und Einflussfaktoren vorwegnehmend zu berücksichtigen. Die in diesem Dokument genannten Maßnahmen und Anforderungen sind in der Regel wie beschrieben umzusetzen.“*
   Die EN 50600 beschreibt ein Vorgehen, um mit Hilfe einer Risikoanalyse zu einem schlüssigen Ergebnis für die bestehenden Risiken zu kommen und daraus eine RZ-Strategie abzuleiten. Ein RZ-Verbund mit Georedundanz stellt dabei einen Spezialfall dar, der das Ergebnis einer Risikoanalyse sein kann. Dieses Vorgehen entspricht dem Vorgehen anderer Normen, wie z.B. der ISO 27001, in der ebenfalls Maßnahmen aus einer Risikoanalyse abgeleitet werden.

   II. Zitat: *„Es besteht ausschließlich dann die Möglichkeit davon abzuweichen, wenn unabweisbare Gründe das erfordern und zugleich ergänzende Maßnahmen ergriffen werden. Diese Maßnahmen müssen geeignet sein, die sich aus der Abweichung eventuell zusätzlichen ergebenden Risiken auf ein akzeptables Niveau zu reduzieren. „Unabweisbar“ meint, dass zwingende technische oder betriebliche Gründe vorliegen. Allein die Tatsache, dass z. B. ein geringerer Abstand zwischen RZ-Standorten einen kostengünstigeren Betrieb ermöglicht, ist nicht als unabweisbar anzusehen.“*
   Aus Sicht des GK 719 ist diese Vorgehensweise mindestens fragwürdig. Das Ergebnis einer Risikoanalyse und die daraus resultierenden Maßnahmen können nicht pauschal für alle Rechenzentren vorweggenommen werden.

4. In Abschnitt 2 werden Umgebungsbedingungen beschrieben, die im Rahmen einer Risikoanalyse zu betrachten sind.
   I. Dieses Vorgehen entspricht grundsätzlich der in EN 50600-2-1 dargestellten Umfeldanalyse für die Standortauswahl. Allerdings verzichtet die Norm auch hier wieder bewusst auf die Festlegung von Werten, da für viele Umfeldeinflüsse das Risiko mit zunehmendem Abstand abnimmt. Die Festlegung eines Wertes unterstellt, dass das Risiko bei geringerem Abstand hoch, bei höherem Abstand dagegen niedrig oder nicht mehr relevant sei. Dabei bleiben aber weitere wesentliche Faktoren und Rahmenbedingungen völlig unberücksichtigt.

   II. Aus Sicht des GK 719 ist nicht nachvollziehbar, warum beispielsweise die in Abschnitt 4.2.2 genannten Abstände der Zertifizierungsunterlagen des TÜV Rheinland aus Sicht des BSI „vernünftige plausible Annahmen“ darstellen.

   III. In Bezug auf die obige Betrachtung ist der erste Absatz im Abschnitt 2.1 daher ebenfalls irritierend:
   Zitat*: „Im Folgenden werden Orte benannt, von denen eine besondere Gefährdung ausgeht. Zu diesen werden nachfolgend Abstandswerte genannt. Sie sind als dringende Empfehlung zu betrachten, die ohne zwingenden unabweisbaren Grund nicht unterschritten werden sollten.“*
   Irreführend ist hier die Formulierung „ohne zwingenden unabweisbaren Grund“, da es einerseits um eine „dringende Empfehlung“ handelt, und es andererseits eigentlich ausreichen sollte, wenn die Risikoanalyse auch bei geringeren Abständen kein Risiko für das betrachtete Rechenzentrum ausweist.

   IV. Im Abschnitt 2.1.4 wird ohne konkrete Ableitung folgende Forderung gestellt: Zitat*: „Zu oberirdischen Bahntrassen mit der Möglichkeit des Güterverkehrs sowie zu öffentlichen Straßen, die für Gefahrgut-Transporte uneingeschränkt freigegeben sind, ist wegen der dort bestehenden Möglichkeit von Unfällen mit Gefahrgut-Transporten ein Mindestabstand von 1.000 m einzuhalten“*.
   Die Vorgehensweise nach EN 50600 ist, das Risiko zu erkennen und durch geeignete Schutzmaßnahmen auf das akzeptable Maß zu reduzieren. Dies kann durch bauliche, technische oder organisatorische Maßnahmen erfolgen.

5. Im Abschnitt 3.3 werden folgende Abstände genannt: Zitat*: „Da es aber, insbesondere durch den Blick in die Vergangenheit, nicht möglich ist, zukünftige potentiell schädliche Situationen und Ereignisse ausreichend sicher vorherzusagen, sollten einander Georedundanz gebende RZ einen Mindestabstand von ca. 200 km zueinander haben. Ist im Einzelfall ein deutlich geringerer Abstand unabweisbar, ist diese Notwendigkeit*

schriftlich ausführlich darzulegen und einer Risikoanalyse zu unterziehen. Keinesfalls sollen georedundante RZ weniger als 100 km voneinander entfernt liegen.“ Zur Motivation der genannten 200 km wird auf den Abschnitt 4.2.7 verwiesen, der verschiedene Autoren zitiert, die aber jeweils andere Entfernungen nennen (3,5 bis mehrere 100 km, mehr als 5.000 km). Aus Sicht des GK 719 und der Anwender fehlt hier die Ableitung für

I. die genannten „ca. 200 km“,
II. die „Notwendigkeit schriftlich ausführlich darzulegen“, warum ein deutlich geringerer Abstand ausreichend sein kann, und
III. „keinesfalls“ weniger als 100 km notwendig sind.

Stattdessen sollte eine qualifizierte Risikoanalyse als Ergebnis ausweisen, ob gemeinsame Risiken für geplante, georedundante Standorte vorliegen – unabhängig von deren Abstand.

6. Im Abschnitt 3.5 wird folgende Anforderung zur Energieversorgung beschrieben: Zitat*: „Innerhalb eines Netzsegmentes der obersten Netzebene (380 kV-Netz) darf sich maximal eines der sich Georedundanz gebenden RZ befinden. Abweichungen hiervon sind dann zulässig, wenn bei einer aus drei oder mehr RZ bestehenden Redundanzgruppe maximal zwei RZ im gleichen Netzsegment liegen und für beide RZ eine redundante eigensichere Notstromversorgung für mindestens 120 Stunden Volllast-Dauerbetrieb sichergestellt ist. Hierfür ist es unerheblich, ob die Einspeisung vom EVU im Stich oder im Ring erfolgt.“* Aus Sicht des GK 719 ist das Management der obersten Netzebene unter der Verantwortung der Netzbetreiber und unterliegt nicht der Einflussmöglichkeit des RZ-Betreibers. Deshalb müssen als Ergebnis der Risikoanalyse geeignete Maßnahmen getroffen werden. Es muss vermieden werden, dass die Stromversorgung des Rechenzentrums unterbrochen wird. Auch die notwendige Autonomiezeit der Notstromversorgung ist ein fundamentaler Bestandteil der Risikoanalyse und kann nicht pauschalisiert werden.

Das GK 719 lädt das BSI ein, sich an der Entwicklung der EN 50600 im deutschen, nationalen Gremium zu beteiligen. Aus Sicht des Gremiums erwarten die Anwender in Deutschland einheitliche und widerspruchsfreie Vorgaben für Rechenzentren. Dies schließt selbstverständlich die Möglichkeit ein, für bestimmte Anwender weitergehende Empfehlungen auf Basis von EN 50600 zu formulieren.

In eigener Sache:
Die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE ist im Rahmen des Normungsvertrages zwischen der deutschen Bundesregierung und DIN Deutsches Institut für Normung e.V. die nationale Plattform für die Erstellung von technischen Normen im Bereich der Elektrotechnik Elektronik und Informationstechnik. Die in den DKE-Gremien aktiven Mitarbeiter werden als Vertreter aller betroffenen und interessierten Fachkreise berufen und repräsentieren die Meinung des entsendenden Fachkreises. In DKE/GK 719 „Rechenzentren“ ist die deutsche Rechenzentrumsbranche mit Experten aus BITKOM, bvfa, eco-Verband der Internetwirtschaft, GDV, VBI, VdTÜV, ZVEI sowie der öffentlichen Hand (z.Z. N.N.) vertreten, die die Interessen von Betreibern, Planern, Herstellern und Anwendern im weitesten Sinne repräsentieren.
Die Normenreihe EN 50600 legt Europa-weit geltende, ganzheitlich formulierte Anforderungen und Empfehlungen für das Design, den Betrieb und die zugehörigen Leistungskennzahlen von Rechenzentren fest und wird unter zwei Normungsaufträgen der EU-Kommission erstellt.