Rechenzentren: Anforderungen an Notstromaggregate steigen weiter

Wenn in Rechenzentren der Strom ausfällt, hat das oft schwere Folgen: Datenverlust und Systemausfälle können Unternehmen erheblichen finanziellen Schaden zufügen. Daher sind Notstromaggregate in Datencentern praktisch unverzichtbar. Je nach Funktion und Bedeutung des Rechenzentrums gelten auch rechtliche Vorgaben, die den Einsatz von Notstromaggregaten faktisch notwendig machen. Diese Regelwerke werden seit 2024 immer weiter verschärft. Eines davon ist die Norm EN 50600. Wer ein Rechenzentrum zertifizieren lassen will, muss nicht nur ein Notstromaggregat haben; dieses muss seit September 2025 auch noch höhere Auflagen erfüllen, denn die EN 50600 wurde überarbeitet. Sie stellt jetzt strengere Anforderungen an die Redundanz und die maximale Umschaltzeit zwischen Netz- und Notstromversorgung.

Betreiber von kritischen Infrastrukturen (KRITIS) sind nach dem BSI-Gesetz (BSIG) und der BSI-Kritisverordnung (BSI-KritisV) verpflichtet, den Betrieb auch bei Stromausfall sicherzustellen. Auch hier wurden erst 2024 die Anforderungen an die Dokumentation und den Nachweis über Wartung und Funktionstests sowie an Informationssicherheits-Managementsysteme verschärft. Der Gesetzentwurf zum KRITIS-Dachgesetz, den das Bundeskabinett im September 2025 beschlossen hat, sieht weitere Vorkehrungsmaßnahmen der Betreiber von Data Centern vor. Daneben können die Anforderungen der NIS-2 Richtlinie auf Basis des deutschen Umsetzungsgesetzes mit extensiven Vorgaben zur Cybersicherheit zum Tragen kommen.

Für die Zertifizierung nach EN 50600 müssen Betreiber zusätzliche Nachweise bereitstellen

Die EN 50600 wurde im August 2025 angepasst. Wer nach EN 50600 zertifiziert werden will oder die Norm als Planungsleitfaden nutzt, muss jetzt seine Notstromversorgung nicht nur technisch sicherstellen, sondern auch die Prozesse, Dokumentation und Nachweise konsequent aufbereiten. Die Norm verlangt nun einen deutlich höheren organisatorischen Aufwand.

Konkret bedeutet das:

- **Klare Verfügbarkeits- und Redundanzanforderungen**
  Betreiber müssen die Dimensionierung ihrer Notstromaggregate genau nachweisen: N+1-Arrangements, Umschaltzeiten, Backup-Kapazitäten. Nicht mehr zulässig sind unklare Interpretationen. Alles muss belegbar sein.
- **Dokumentierte Probeläufe und Tests**
  Regelmäßige Testläufe der Notstromaggregate sind Pflicht. Dabei müssen Lastübernahmezeiten, Betriebsdauer und eventuelle Störungen dokumentiert werden. Die Unterlagen dienen später als Nachweis für Audits und Zertifizierungen.
- **Monitoring und Reporting**
  Notstromaggregate müssen jetzt in die Überwachungs- und Managementsysteme eingebunden sein. Betreiber müssen Verfügbarkeitskennzahlen kontinuierlich erfassen und Ausfälle oder Verzögerungen protokollieren.
- **Integration von Energie- und Umweltaspekten**
  Die Norm fordert, die Energieeffizienz der Notstromversorgung zu berücksichtigen. Betreiber sollten prüfen, ob Dieselaggregate mit ihren Nachhaltigkeitszielen vereinbar sind und Alternativen wie Batteriepuffer oder Hybridlösungen einplanen.

- **Prozessverantwortung & Change-Management**
  Jede Änderung an der Stromversorgung, am Layout der Rechenzentren oder an Betriebsabläufen muss dokumentiert werden. Es müssen Verantwortlichkeiten klar definiert und Eskalationswege für Störungen festgelegt sein.

BSI-Kritisverordnung: Mehr Verantwortung für Betreiber

Neben den technischen Normen verschärfen sich auch die rechtlichen Anforderungen an Betreiber von Rechenzentren nach der BSI-Kritisverordnung. Diese gilt im Bereich der kritischen Infrastruktur, zum Beispiel Telekommunikation, Energie, Finanz- und Gesundheitswesen. Auch die Größe eines Rechenzentrums kann entscheidend sein: Ab einer vertraglich vereinbarten IT-Leistung von mindestens 3,5 MW gelten Anbieter von IT-Infrastruktur als Teil der kritischen Infrastruktur. Diese Betreiber müssen ein hohes Maß an technischer und organisatorischer Resilienz nachweisen, auch im Bereich der Notstromversorgung.

Rechenzentren gelten zunehmend als Teil der kritischen Infrastruktur, weil ihr Ausfall ganze Branchen oder öffentliche Dienste lahmlegen kann.

Durch die Anpassungen im haben sich die Anforderungen spürbar verschärft:

Wesentliche Neuerungen und Anforderungen:

- **Längere Überbrückungszeit:** Für KRITIS-Rechenzentren gilt inzwischen die Vorgabe, dass die Stromversorgung im Notfall mindestens 24 Stunden, häufig aber auch deutlich länger (bis 48 oder 72 Stunden je nach Schutzbedarf) durch Notstromaggregate sichergestellt werden muss.
- **Dokumentations- und Prüfpflichten:** Betreiber müssen regelmäßige Funktionstests und Wartungen ihrer Notstromanlagen durchführen und die Ergebnisse lückenlos dokumentieren. Diese Nachweise sind Grundlage für Audits und behördliche Prüfungen.
- **Redundanz und Auslastung:** Rechenzentren dürfen ihre Systeme nicht permanent unter Volllast betreiben. Die Infrastruktur muss so ausgelegt sein, dass Ausfälle einzelner Komponenten durch andere kompensiert werden können (z. B. N+1-Redundanz).
- **Risikomanagement und Notfallplanung:** Betreiber müssen Risikoanalysen, Notfall- und Wiederanlaufpläne vorhalten und regelmäßig aktualisieren, inklusive klar definierter Verantwortlichkeiten.
- **Informationssicherheits-Managementsystem (ISMS):** KRITIS-Betreiber müssen ein ISMS nach dem Stand der Technik implementieren und regelmäßig durch unabhängige Prüfer auditieren lassen.
- **Gebäude- und Standortanforderungen:** Neben der IT-Infrastruktur gelten auch Anforderungen an Bauweise, Brandschutz, physische Sicherheit und Standortkriterien. Das BSI hat hierzu eigene Leitfäden und Mindestabstände definiert, die bereits bei der Planung neuer Rechenzentren berücksichtigt werden sollten.
- **Integration mit Energieversorgung und Netzsicherheit:** Die Vorgaben aus der BSI-Kritisverordnung sind eng mit dem Energiewirtschaftsgesetz (EnWG, §§ 11 ff.) verzahnt und verlangen eine sichere und redundante Anbindung an das Stromnetz.

Mit dem KRITIS-Dachgesetz werden weitere Verpflichtungen kommen

Das geplante KRITIS-Dachgesetz setzt die CER-Richtlinie (EU) 2022/2557 in deutsches Recht um und stärkt die physische und organisatorische Resilienz kritischer Anlagen, unter anderem Risikoanalysen, Notfall- und Wiederanlaufpläne, Meldewege. Es ergänzt damit die BSI-Kritisverordnung/BSIG (cyberbezogene Pflichten und anlagenbezogene Schwellen). Einen Entwurf des Gesetzes hatte das Bundeskabinett im September 2025 beschlossen. Das sind die Eckpunkte des KRITIS-Dachgesetzes:

- **Erweiterte Nachweis- und Berichtspflichten:** Betreiber sollen Risikoanalysen durchführen, Resilienzmaßnahmen festlegen und Störungen melden.
- **Verpflichtendes Resilienzmanagement:** Der Entwurf des KRITIS-Dachgesetzes schreibt unter anderem Notfall- und Wiederanlaufpläne sowie organisatorische Zuständigkeiten zur Aufrechterhaltung des Betriebs bei Ausfällen vor.
- **Verzahnung mit europäischen Zielen:** Der Gesetzentwurf berücksichtigt auch übergreifende EU-Ziele wie Klimaschutz, Nachhaltigkeit und Energieeffizienz. Zwar nennt weder die CER-Richtlinie noch das Dachgesetz konkrete Effizienzwerte für Notstromaggregate, sie erwarten aber, dass Betreiber angemessene und nachhaltige technische Lösungen einsetzen. Dazu zählen etwa:

  - Prüfung alternativer oder emissionsärmerer Kraftstoffe,
  - Kombination klassischer Dieselaggregate mit Batterie- oder Hybridlösungen,
  - Maßnahmen zur Reduktion von Emissionen und Energieverlusten.

- **Digitalisierung und Fernüberwachung:** Künftig können Betreiber den Zustand ihrer Energieversorgungssysteme – insbesondere Notstromaggregate – digital erfassen, überwachen und dokumentieren. Automatisierte Überwachung und Fernsteuerung gelten als Stand der Technik und werden zunehmend als Nachweis für Resilienz und Reaktionsfähigkeit erwartet.

Versorgungssicherheit und Nachhaltigkeit: Hybridlösungen im Fokus

Immer häufiger setzen Rechenzentren auf hybride Stromversorgungslösungen, die konventionelle Generatoren und Energiespeichersysteme mit nachhaltigen Energiequellen wie Solar- und Windkraft kombinieren. So werden fossile Brennstoffe reduziert und langfristig auch Betriebskosten und CO?-Emissionen deutlich gesenkt. Der Vorteil liegt auf der Hand: Unternehmen erhöhen den Anteil erneuerbarer Energien im laufenden Betrieb und sichern sich mit klassischen Notstromaggregaten ab. Bei Stromausfällen oder Netzschwankungen stehen dann auch Diesel- oder Gassysteme zur Verfügung.

Die Integration erneuerbarer Energien bringt jedoch auch Herausforderungen mit sich: Der Strombedarf in Rechenzentren ist rund um die Uhr konstant, während Wind- und Solaranlagen wetterabhängig schwanken. Diese Spannung zwischen dauerhaftem Verbrauch und volatiler Erzeugung bleibt eine der größten Aufgaben bei der Energiewende in der IT-Infrastruktur.

Gelingt die Integration, können Betreiber jedoch ihre CO?-Bilanz verbessern und gleichzeitig langfristig ihre Energiekosten senken, ohne Kompromisse bei der Versorgungs- und Betriebssicherheit eingehen zu müssen. Stromaggregate bleiben dabei als Backup-Systeme unverzichtbar und sorgen für maximale Ausfallsicherheit, wenn die erneuerbaren Quellen nicht verfügbar sind.

Abwärmenutzung: Energie clever verwerten

Ebenfalls finanziell interessant ist die Nutzung der Abwärme, die in Rechenzentren kontinuierlich entsteht. Sie kann in Nah- oder Fernwärmenetze eingespeist werden, Gebäude heizen oder Warmwasser bereitstellen. So können Unternehmen Betriebskosten senken und neue Einnahmequellen schaffen. Gleichzeitig unterstützt die Nutzung der Abwärme die Reduktion von CO?-Emissionen. Daher soll sie künftig auch gesetzlich verpflichtend werden: Ab Mitte 2026 sollen Rechenzentren nach dem neuen Energieeffizienzgesetz mindestens 10 Prozent ihrer Abwärme weiterverwenden, mit einer geplanten Steigerung auf 20 Prozent bis 2028.

Fazit

Die Anforderungen an Notstromaggregate in Rechenzentren sind in den letzten Jahren erheblich gestiegen. Getrieben wurde diese Entwicklung durch neue gesetzliche Vorgaben, normative Standards und das steigende gesellschaftliche wie politische Interesse an Versorgungssicherheit, Resilienz und Nachhaltigkeit. Insbesondere die Überarbeitung der EN 50600 sowie die novellierte BSI-Kritisverordnung markieren einen Paradigmenwechsel im Verständnis von Betriebssicherheit und Notfallvorsorge in der digitalen Infrastruktur.

Zukünftige Regulierungen auf EU-Ebene werden diesen Trend weiter verstärken und insbesondere die physische und technische Resilienz von Datencentern stärker in den Fokus rücken. Betreiber müssen sich darauf einstellen, nicht nur technische Mindestanforderungen zu erfüllen, sondern auch umfassende Nachweise über Wartung, Effizienz, Umweltverträglichkeit und Sicherheitsmanagement zu erbringen.

Die Integration hybrider Systeme aus klassischen Notstromaggregaten und perspektivisch Batteriespeichern ist eine zukunftsfähige Lösung, die sowohl die Betriebssicherheit erhöht als auch ökologische und ökonomische Vorteile bietet. Auch die Nutzung der Abwärme, die für neue Rechenzentren verpflichtend wird, könnte für einige Unternehmen finanziell attraktiv sein.

Insgesamt stehen Rechenzentrumsbetreiber vor der Herausforderung, ihre Notstromversorgung nicht nur an gestiegene rechtliche Anforderungen, sondern auch an technologische und nachhaltige Standards anzupassen. Die Modernisierung von Notstromlösungen wird daher ein zentraler Baustein jeder zukunftsorientierten Rechenzentrumsstrategie sein, mit dem Ziel, Ausfallsicherheit, Energieeffizienz und Klimaverträglichkeit in Einklang zu bringen.

Ansprechpartner:

Marc Goldberg
Tel: +49 211 4155597 976
marcgoldberg@kpmg-law.de

Dirk-Henning Meier
Tel:

Francois Heynike, LL.M. (Stellenbosch)
Tel: +49-69-951195770
fheynike@kpmg-law.com