KAMP


# HOCHVERFÜGBAR? SICHER? PERFORMANT?

IT-Verfügbarkeit in Unternehmen kann man planen.

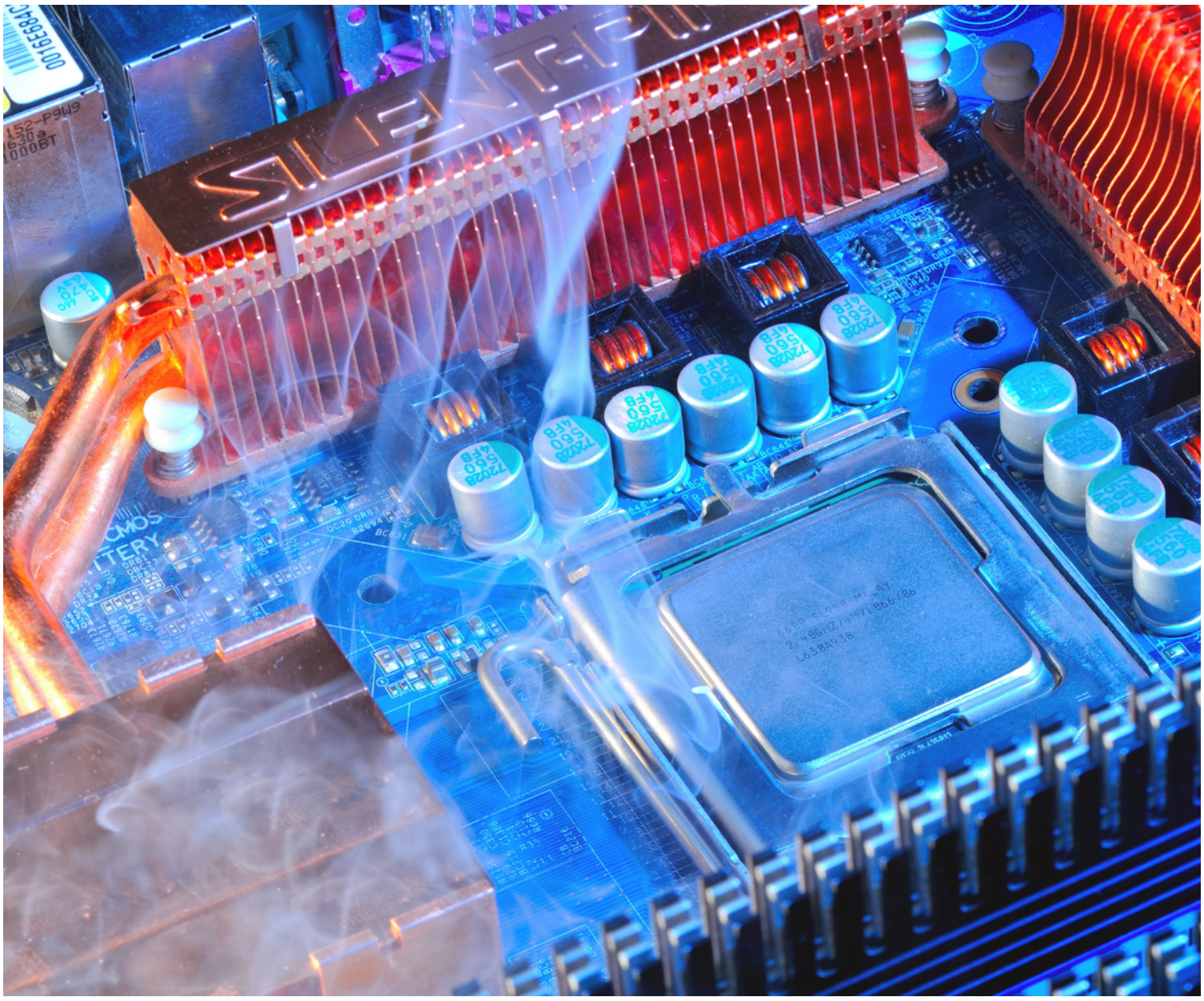
DIN ISO/IEC 27001 ZERTIFIZIERT
IT-SICHERHEIT 27002 GEPRÜFT
CLOUD-DIENSTE 27018 GEPRÜFT
DIN EN ISO 9001 ZERTIFIZIERT
RECHENZENTRUM ECB•S ZERTIFIZIERT
DEUTSCHER RECHENZENTRUMSPREIS 2014
3. PLATZ KATEGORIE 10: GESAMTHEITLICHE ENERGIEEFFIZIENZ IM RZ

# WENN DIE IT AUS DER ROLLE FÄLLT

„... Im Siegerland ist das komplette Telefonnetz ausgefallen. Datenleitungen waren unterbrochen, Internet und Mobilfunk gestört. Bis zum Nachmittag waren Polizei und Feuerwehr nur über Handy-Nummern zu erreichen. Inzwischen funktioniert die Notruf-Nummer 110 wieder“, so beschreibt Stefan Michel aus dem WDR2-Studio die Situation im Siegerland am 21. Januar 2013.

Rund 90.000 Menschen erlebten im Kreis Siegen, wie sehr die Informationstechnologie bereits unseren Alltag bestimmt: Nach einem Brand im Gebäude der Deutschen Telekom war es zu einem Störfall mit erheblichen Folgen gekommen. Krankenhäuser, Behörden und Firmen waren vom Telefon- und Datennetz abgeschnitten. An Tankstellen bildeten sich Schlangen, weil Fahrer bereits betankter Wagen plötzlich nicht mehr mit ihrer EC-Karte zahlen konnten. Sparkassen und Volksbanken mussten Filialen schließen, weil ihre Systeme keine Verbindungen zu den jeweiligen Rechenzentren mehr hatten. Einen Störfall mit massiven Auswirkungen gab es auch im September 2017, als ein Brand im Kölner WDR-Gebäude den gesamten Betrieb des Senders behinderte. Bei einer Überprüfung der Notstromversorgung des Gebäudes fingen über 200 Batterien Feuer. Um den Brand zu löschen, musste der Batterie-Raum mit einem speziellen Schaum geflutet werden. Neben Unterbrechungen im Rundfunkprogramm führte der Brand sogar zu massiven Störungen im täglichen WDR-Abendfernsehprogramm.

Die Basis für viele Kommunikations- und Business-Prozesse bildet heutzutage die Informationstechnologie. Ohne IT-Unterstützung wird kaum eine Geschäftstätigkeit oder Unternehmensprozess abgewickelt. Fallen IT oder Teile der Datenkommunikation aus, so ist dies in der Regel nicht nur mit unvorhergesehenen, hohen Kosten, sondern auch mit dem Verlust von Marktanteilen und Image verbunden. Längere Ausfälle können die gesamte Existenz des Unternehmens gefährden. Gegen Störungen, die aufgrund höherer Gewalt oder mutwillig durch Sabotage herbeigeführt werden, können sich Unternehmen nur schwer schützen. Um so mehr gilt es, für diese Fälle Vorsorge zu treffen.



# RISIKEN MINIMIEREN, IT-AUSFÄLLE VERMEIDEN

Notfallplanung wird in vielen Unternehmen noch stiefmütterlich behandelt. Die meisten kleinen und mittleren Unternehmen machen sich erst Gedanken, wenn die Störung bereits eingetreten ist. Dabei ist es notwendig, rechtzeitig ein Bewusstsein für mögliche Risiken zu entwickeln. Die Ursachen für Ausfälle der IT in Unternehmen können vielfältig sein: Viren oder Würmer, fehlerhafte Soft- und Hardware, schlechte Wartung, Stromausfälle oder auch menschliches Fehlverhalten sind nur einige Beispiele. Für die Notfallplanung müssen daher sowohl technische als auch organisatorische und kommunikative Maßnahmen und Abläufe festgelegt werden, damit die Rahmenbedingungen für eine hochverfügbare IT-Infrastruktur greifen. Auch bereits bestehende Notfallpläne sollten regelmäßig aktualisiert und geprüft werden. Um die Risiken, die durch einen IT-Ausfall ausgelöst werden können, gering zu halten, empfiehlt es sich, die notwendige Verfügbarkeit der vorhandenen IT-Systeme genau zu analysieren:

- Welche Prozesse sind in meinem Unternehmen von der IT abhängig?
- Welche Anwendung ist besonders schutzbedürftig?
- In welchem Zeitraum muss die Anwendung nach einem Störfall wieder zur Verfügung stehen?
- In welchem Zeitraum muss die Anwendung wieder über das Netzwerk erreichbar sein?
- Über welchen Zeitraum kann die Anwendung im eingeschränkten Betrieb betrieben werden?
- Habe ich Maßnahmen ergriffen, um IT-Ausfälle zu vermeiden?

Ist ein Unternehmen sehr stark von der IT abhängig, muss es rechtzeitig eine Strategie entwickeln, um Störungen zu verhindern oder schnell zu überwinden. Zu klären sind dabei viele Fragen: Wie kann ich die Hochverfügbarkeit meiner IT-Systeme gewährleisten? Welche physischen, technischen und personellen Kapazitäten benötige ich dafür? Sind gegebenenfalls bauliche Maßnahmen erforderlich, um der IT-Infrastruktur ein Umfeld zu geben, in der hochsensible Geräte effizient betrieben werden können? Muss ich zum Schutz der Systeme zusätzlich in Hardware und Software investieren? Ist meine IT vor äußeren Zugriffen hinreichend gesichert? Sollten die eigenen personellen, räumlichen, technischen oder auch fachlichen Ressourcen nicht ausreichen, besteht die Option, die IT – komplett oder in Teilen – an einen spezialisierten Provider auszulagern.

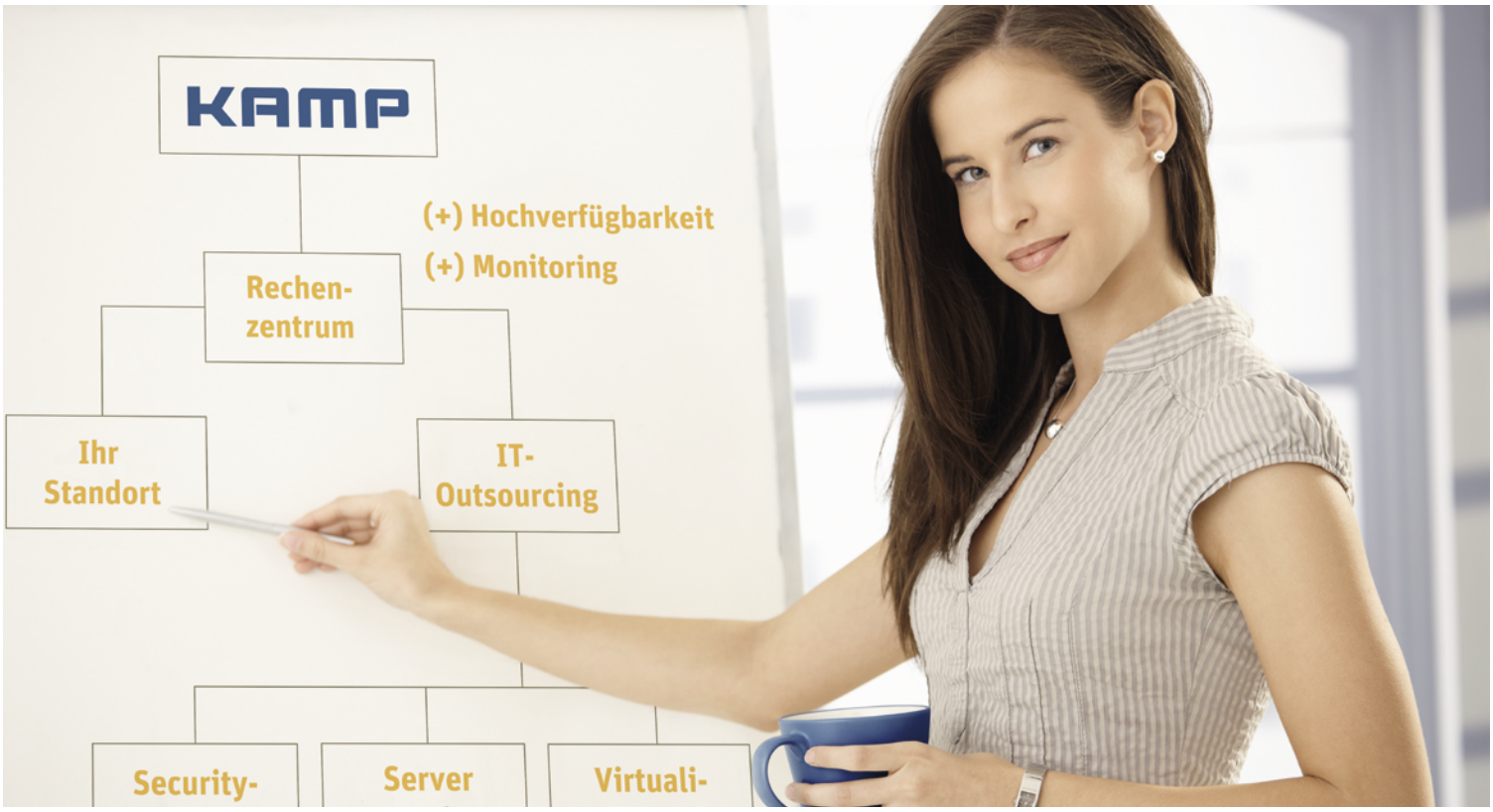
# COLOCATION – DIE SICHERE BASIS FÜR IT

Durch Colocation in einem zertifizierten Rechenzentrum behalten Unternehmen die Hoheit über Hardware und Daten und profitieren von einer IT-Infrastruktur für höchste Ansprüche.

Der hohe Infrastruktur-Standard, den professionelle IT-Dienstleister ihren Kunden im Bereich von Colocation-Services bieten können, lässt sich am eigenen Standort nur mit enorm hohen Unternehmens-Investitionen realisieren. IaaS-Dienste sicherheitszertifizierter Rechenzentrumsbetreiber bieten hingegen individuelle Lösungen, die mit Transparenz und effizienter Kosten-Nutzen-Kalkulation punkten können. Gleichzeitg unterstützt ein Deligieren der Infrastruktur-Verantwortung die Konzentration auf die Kerngeschäfte.


**IaaS und Colocation im ISO-zertifizierten KAMP-Rechenzentrum:**

- **KAMP DHP:** Der ISO-konforme Einstieg in die Cloud für Unternehmen, die ein virtualisiertes Datacenter mit skalierbaren Hardwareressourcen und hohem Datenschutz suchen.
- **KAMP DHP Enterprise:** Mit der umfangreichen Cloudlösung realisieren Unternehmen große IT-Projekte auf einer dynamisch skalierbaren IaaS-Plattform. Hohe Performance und garantierte SLAs, verbunden mit den Kosten- und Flexibilitätsvorteilen einer dynamischen Cloud, zeichnen DHP Enterprise aus. Ideal auch in Kombination mit einem Private-Rack oder einer Private-Suite.
- **KAMP Private-Rack:** Betreiben Sie beim Server-Housing Ihre eigene Hardware in einem oder mehreren Racks im KAMP-Rechenzentrum. Wählen Sie aus einer Vielzahl an Konfigurationsmöglichkeiten wie eigenem Schließsystem, unterschiedlichen Brandabschnitten oder Hands-On-Services.
- **KAMP Private-Suite:** Hochsensible IT verlangt nach der größeren physikalischen Sicherheit einer eigenen und baulich separierten Rechenzentrumsfläche. Eine KAMP Private-Suite vereint eine schlüsselfertige technische Infrastruktur mit räumlicher Eigenständigkeit, modernsten Sicherheitsmaßnahmen und SLA-garantierten Verfügbarkeiten.


# DAS KONZEPT DER REDUNDANZ

Wie stellt KAMP die Verfügbarkeit seiner IT-Dienstleistungen sicher? KAMP setzt auf das Prinzip der Redundanz. Der Grundgedanke lautet: Wird ein Service oder eine Dienstleistung durch einen Störfall unterbrochen, so ist im Gesamtsystem ein Plan B vorgesehen, der automatisch umgesetzt wird, um den Service weiterführen zu können.

Ein Teil des Redundanz-Modells ist darauf ausgelegt, Komponenten (Festplatten, Server, Speicher, Netzteile, Switche, Router), Server oder Ressourcen doppelt vorzuhalten und einzusetzen. Das beginnt bereits bei der „Vorratshaltung“ von Qualitäts-Hardware oder Ersatzteilen, damit sie im Notfall nicht erst aufwendig bestellt und angeliefert werden müssen, sondern jederzeit für den Einsatz griffbereit sind. Hochverfügbarkeit hat hier ihren Preis. Das Sicherheitsdenken zahlt sich aber aus, wenn Downtimes dadurch so gering wie möglich gehalten werden.

### Die intelligente Steuerung

Der weitaus größere Teil beim redundanten Aufbau von IT-Strukturen macht die intelligente Planung eines möglichen Ausfallszenarios aus. Redundante IT-Systeme basieren auf einem detaillierten Konzept und einem logischen Aufbau. Dabei wird festgelegt, welche Komponente wann und wie einspringt, um bei einem Ausfall die Funktion der gestörten oder defekten Einheit zu übernehmen.

**Beispiel:** Ein Automobilzulieferer fertigt seine Bauteile on Demand auf Bestellung der Automobilindustrie. Dem IT-Leiter ist bewusst, dass die Datenkommunikation, über den der Bestellprozess läuft, nicht ausfallen darf. Er entscheidet, eine weitere Datenanbindung für sein Fertigungswerk in Auftrag zu geben. Fällt eine Verbindung aus, kann die Kommunikation über die zweite Strecke weiterlaufen. Mehrere Fragen gilt es nun zu klären. Reicht es aus, eine Anbindung, die auf gleicher Technologie basiert, zweimal vorzuhalten? Oder sollte der IT-Leiter nicht besser zwei unterschiedliche Zugangstechnologien für seine Anbindung auswählen? Ist die Primäranbindung beispielsweise kupferbasiert, können mobile Datennetze, Glasfaser oder Richtfunk als Alternativen für die zweite Anbindung in Betracht gezogen werden. Laufen die Daten beim selben Provider auf? Dann ist unter Umständen eine Provider-Redundanz notwendig. Die Fragen machen deutlich, dass sich hinter dem Konzept der Redundanz mehr verbirgt als die bloße Aussage „Doppelt hält besser“!

### Qualität macht sich bezahlt

Das Redundanzkonzept muss zielgenau auf die Bedürfnisse des Kunden zugeschnitten sein. Intensive Beratung, technisches Know-how und finanzielle Aufwendungen in Hard- und Software sind notwendig, um die Hochverfügbarkeit der IT-Systeme zu gewährleisten. Die Investitionen lohnen sich spätestens dann, wenn Geschäftsprozesse durch eine Störung nicht unterbrochen werden. Jetzt macht es sich bezahlt, dass die IT-gesteuerten Prozesse über alternative Komponenten oder redundante Wegeführung gemanaged werden, Ausfallzeiten gänzlich vermieden oder so gering wie möglich gehalten werden und keine unkalkulierbaren Kosten entstehen. KAMP setzt mit dem Konzept der Redundanz darauf, dass eine Störung der IT systemimmanent aufgefangen werden kann und garantiert in den Produkt-SLAs eine Hochverfügbarkeit von bis zu 99,9 Prozent.

## Haben Sie noch Fragen – wir sind gerne für Sie da!

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91
46117 Oberhausen

Fon +49 (0) 208.89 402-35
Fax +49 (0) 208.89 402-40

info@kamp.de
www.kamp.de

DIN ISO/IEC 27001 ZERTIFIZIERT
CLOUD-DIENSTE 27018 GEPRÜFT
IT-SICHERHEIT 27002 GEPRÜFT
DIN EN ISO 9001 ZERTIFIZIERT
RECHENZENTRUM ECB•S ZERTIFIZIERT

KAMP

00501811