Ein Unternehmen der

enviaM-Gruppe

Whitepaper

Datacenter Leitfaden: Fünf Schritte zur sicheren Rechenzentrums-Wahl

Inhalt

1 Die Vorteile bei der Auslagerung Ihrer Server

1.1 Herausforderung „eigenes Rechenzentrum“

IT-Systeme stehen heute unter Druck: Sie sollen flexibel wachsen, höchste Sicherheitsstandards erfüllen und laufend neue Anforderungen wie EnEfG, NIS2 oder KRITIS umsetzen. Viele Unternehmen betreiben trotzdem eigene Rechenzentren – und stoßen dabei zunehmend an Grenzen. Ausfälle häufen sich, Sicherheitsrisiken nehmen zu, und qualifiziertes Personal fehlt. Gleichzeitig wachsen die gesetzlichen und technischen Anforderungen. Die entscheidende Frage lautet nicht mehr, **ob** Unternehmen ihre IT neu aufstellen sollten – sondern **wie** sie es am besten tun.

1.2 Zentrale Vorteile externer Rechenzentren

- **Geringeres Ausfallrisiko bei gleichzeitiger Sicherung der Geschäftskontinuität:**
  Externe Rechenzentren bieten Hochverfügbarkeit, technische Redundanz und professionelles Personal. Dadurch reduzieren Sie Downtimes und vermeiden finanzielle Verluste.

- **Skalierbarkeit und Kosteneffizienz:**
  Flexibel anpassbare Ressourcen (Pay-per-use) vermeiden Überkapazitäten oder Engpässe, besonders relevant, wenn Ihr Unternehmen saisonalen Schwankungen unterliegt oder stark wächst.

- **Fachkräftemangel überbrücken:**
  Die IT-Expertise externer Anbieter hilft, interne Defizite zu kompensieren. Durch Services wie Remote Hands können Sie bei Bedarf auf spezialisierte Fachkräfte zugreifen, ohne selbst einstellen zu müssen.

- **Edge-Computing für Echtzeitanwendungen:**
  Durch die lokale Verarbeitung von Daten reduzieren Sie Latenzzeiten und senken Übertragungskosten – ideal für IoT, Produktion oder Smart Services.

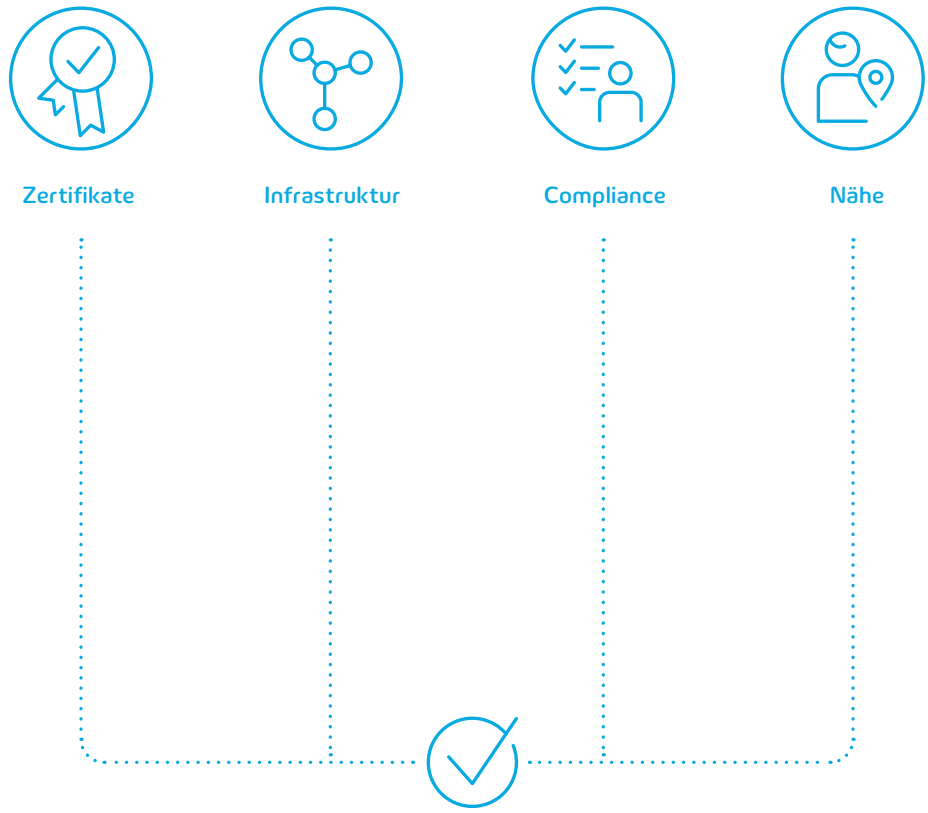
- **Energieeffizienz und Nachhaltigkeit (EnEfG):**
  Externe Anbieter setzen regulatorische Vorgaben (PUE-Werte, Abwärmenutzung, Grünstrompflicht) schneller und wirtschaftlicher um als interne IT-Abteilungen.

- **Moderne Sicherheitsstandards:** Professionelle Rechenzentren bieten zertifizierte physische, logische und organisatorische Sicherheit (z. B. ISO 27001, EN 50600), inklusive Schutz vor Cybercrime, Naturkatastrophen und menschlichen Fehlern.

- **Rechtssicherheit durch Standortwahl (Deutschland/EU):**
  Lokales Housing kann vor Zugriff durch außereuropäische Behörden (z. B. durch den US CLOUD Act) schützen und DSGVO-Konformität sichern.

1.3 Handlungsempfehlung bei der Anbieterauswahl

- **Überprüfen Sie relevante Zertifizierungen**
  (z. B. ISO 27001, DIN EN 50600) als Mindeststandard.
- **Evaluieren Sie Anbindung und Infrastruktur**
  (Glasfaser, Redundanz, Cloud-Connect etc.), sie müssen zur Größe und den Anforderung Ihres Unternehmens passen.
- **Evaluieren Sie Compliance-Anforderungen**
  (NIS2, KRITIS) entsprechend Ihrer Branche.
- **Berücksichtigen Sie geografische Nähe und persönlichen Kontakt.**
  Beides stärkt Vertrauen und erhöht Ihre Reaktionsfähigkeit.



Grafik: Leitfaden für die Anbieterwahl – Fokus auf Zertifizierungen, Anbindung, Compliance und persönliche Kontaktmöglichkeiten

1.4 Fazit

Der Betrieb eines eigenen Rechenzentrums ist für viele Unternehmen weder wirtschaftlich noch zukunftsfähig. Mit der Auslagerung Ihrer IT-Strukturen in ein externes zertifiziertes Datacenter gewinnen Sie Flexibilität, Sicherheit, Kostentransparenz und Entlastung – und einen nachhaltigen Erfolgsfaktor in einer zunehmend digitalen Wirtschaft.

Moderne Geschäftsprozesse und digitale Wertschöpfungsketten stellen das Rechenzentrum in den Mittelpunkt unternehmerischer Leistungsfähigkeit. Vernetzte Kommunikation, Data Analytics auf Basis von Echtzeitwerten und intelligente Prozesse erfordern ein leistungsstarkes Datacenter. Doch genau hier haben viele Unternehmen noch immer Nachholbedarf. Hohe Ausfallraten, eingeschränkte Connectivity und unzureichende Performance während Auslastungsspitzen werden vielerorts zur Gefahr für den operativen Betrieb. IT-Infrastrukturen werden zudem immer komplexer. Um sie zu betreiben, braucht es IT-Qualifikationen auf höchstem Niveau. Die schnelle technologische Entwicklung und die sich permanent ändernden Anforderungen an IT-Sicherheit und Datenschutz erfordern, dass IT-Wissen permanent aktualisiert wird und neue Rechtsgrundlagen zeitnah umgesetzt werden.

In vielen Unternehmen zählt IT aber nicht zum Kerngeschäft und die notwendigen Kompetenzen sind intern nicht immer in vollem Umfang vorhanden. Der Umgang mit den Anforderungen an die eigene IT-Infrastruktur wird dann schnell zum Balanceakt. Trotzdem geben in einer Umfrage des Bitkom e. V. noch 55 % der befragten Unternehmen an, ein eigenes Rechenzentrum zu betreiben[1], auch wenn der Trend sich bereits verschiebt[2,3].

Dabei ist die Verlagerung einzelner IT-Komponenten bis hin zur Auslagerung der gesamten IT-Infrastruktur in ein externes Datacenter eine kostengünstige und gleichzeitig sichere Möglichkeit den Anforderungen an IT-Sicherheit und Datenschutz gerecht zu werden. Doch wie findet man den passenden Datacenter-Anbieter und welche Kriterien zeichnen einen seriösen Dienstleister aus?

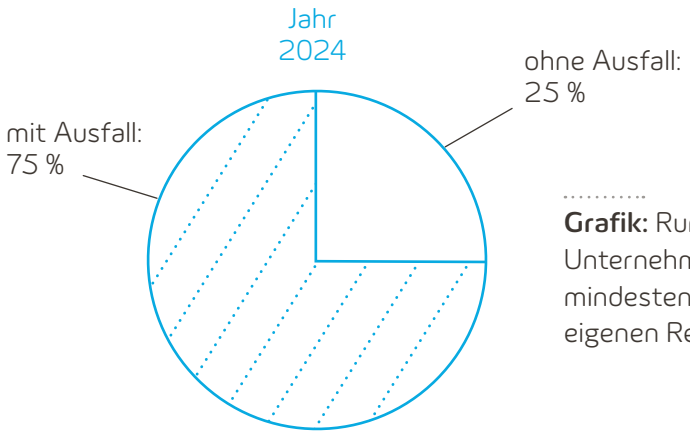
Mit diesem Whitepaper

erhalten Sie eine Übersicht über die Vorteile der Auslagerung von IT-Infrastrukturen in ein externes Rechenzentrum sowie praktische Tipps und sofort einsetzbare Checklisten – damit Sie die richtige Entscheidung für Ihr Unternehmen treffen.

2 Wechseln und gewinnen: Wie Sie Ihr Unternehmen mit einem externen Datacenter stärken

2.1 Sie vermeiden Ausfälle und finanzielle Verluste

Drei Viertel der Unternehmen in der DACH-Region haben im vergangenen Jahr Ausfälle in ihren Rechenzentren erlebt[4], oft mit erheblichen finanziellen Folgen in Millionenhöhe. Downtimes und Performance-Probleme fügen nicht nur direkten Schaden zu, sondern beeinträchtigen auch die Reputation. Ein externes Rechenzentrum mit hoher Verfügbarkeit, technischer Redundanz und erfahrenem Betriebsteam minimiert das Risiko solcher Ausfälle und sorgt für stabile IT-Prozesse. So sichern Sie Geschäftskontinuität und vermeiden teure Betriebsunterbrechungen.



Grafik: Rund 75 % der befragten Unternehmen hatten im letzten Jahr mindestens einen Ausfall in ihrem eigenen Rechenzentrum verzeichnet[4].

2.2 Sie gehen mit der Zeit

Immer mehr Unternehmen verlagern ihre IT in externe Rechenzentren oder die Cloud. Gartner prognostiziert, dass schon in 2025 bis zu 80 % der bislang firmeneigenen Rechenzentren ausgelagert werden[3,5]. Immer weniger Unternehmen planen, ausschließlich auf eigene IT-Infrastruktur zu setzen[3]. 89 % der Unternehmen in Deutschland nutzen inzwischen Cloud-Services, was die Auslagerung von IT-Infrastrukturen an externe Rechenzentren vorantreibt[2].

Auch Colocation-Angebote, das Mieten von physischer Infrastruktur in einem externen, professionellen betriebenen Rechenzentrum, gewinnen an Bedeutung: 31 % der deutschen Firmen planen, künftig mehr Colocation-Ressourcen zu nutzen. Die Vorteile liegen auf der Hand: Moderne externe Rechenzentren bieten einfache Skalierbarkeit, hohe Sicherheitsstandards, Kosteneffizienz und entlasten das eigene IT-Personal[6]. Durch diese Vorteile können Unternehmen agiler und widerstandsfähiger agieren.

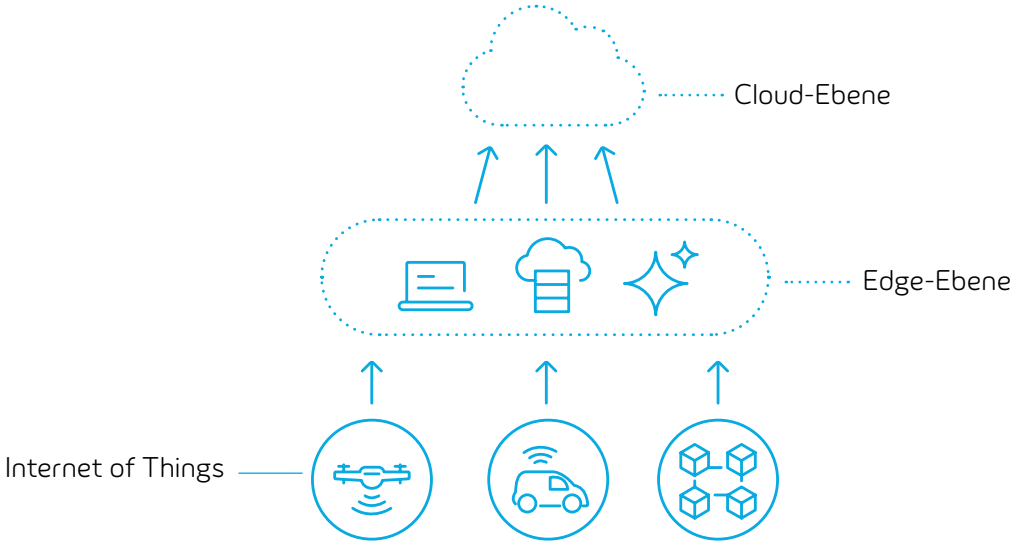
Sie profitieren von Datenverarbeitung in Echtzeit dank Edge-Computing

Edge-Computing bezeichnet die Verarbeitung von Daten in unmittelbarer räumlicher Nähe des Ortes, an dem sie entstehen. Die Daten müssen nicht erst an eine weit entfernte Cloud versendet werden. Die Datenspeicherung und die Rechenkapazitäten befinden sich stattdessen beispielsweise in einem lokalen Rechenzentrum.

Edge-Computing entwickelt sich zu einem entscheidenden Erfolgsfaktor für Unternehmen. Laut IDC stiegen die Investitionen in Edge-Lösungen in den letzten Jahren im zweistelligen Prozentbereich[7]. Gartner prognostiziert, dass in naher Zukunft weltweit mehr als die Hälfte der Unternehmensdaten durch Edge-Computing und damit außerhalb traditioneller Rechenzentren oder Clouds verarbeitet werden[8].

Unternehmen, die auf Anwendungen in Echtzeit oder die Verarbeitung besonders großer Datenmengen angewiesen sind, profitieren von Edge-Computing. Durch geringe Latenzen ermöglicht es eine effizientere Datenverarbeitung. Außerdem reduziert es die oft hohen Kosten für die Übertragung großer Datenmengen zwischen Endgeräten und Cloud-Infrastrukturen. Besonders relevant ist dies beispielsweise für industrielle IoT-Szenarien in Bereichen wie der Produktion (Smart Factory), der Landwirtschaft (präzise Feldbewirtschaftung) oder der intelligenten Verkehrssteuerung[9].

Weitere Vorteile sind eine höhere Ausfallsicherheit durch lokale Weiterverarbeitung auch bei Netzstörungen sowie die Einhaltung von Datenschutzanforderungen, da sensible Daten am Entstehungsort bleiben können. Hiervon profitieren besonders Produktions- und Einzelhandelsunternehmen, kritische IT-Systeme (KRITIS), sowie Unternehmen aus Branchen mit hohen Sicherheitsanforderungen, wie dem Gesundheitswesen oder den Finanzdienstleistungen.



Grafik: Edge-Computing ermöglicht die lokale Verarbeitung von Daten nahe am Entstehungsort – für geringe Latenzen, niedrigere Übertragungskosten und mehr Ausfallsicherheit.

Durch die lokale Verarbeitung und Speicherung von sensiblen Daten kann Edge Computing Ihrem Unternehmen dabei helfen, Datenschutzanforderungen zu erfüllen [9].

Wenn Ihr Unternehmen bereits eine Cloud-Lösung nutzt, kann Edge Computing nahtlos integriert werden. Ein externes Rechenzentrum mit entsprechender IT-Architektur kann dann als Brücke zwischen Cloud und lokaler Infrastruktur dienen [10].

Die Vorteile von Edge-Computing auf einen Blick

- **Leistung und geringe Latenz**
  Bessere Performance für Echtzeitanwendungen
- **Kostenersparnis**
  Weniger Transitkosten durch lokale Datenverarbeitung
- **Datenschutz & Sicherheit**
  Bessere Einhaltung von Datenschutzgesetzen
- **Ausfallsicherheit**
  IT-Systeme bleiben auch bei Netzwerkausfällen funktionsfähig
- **Flexibilität**
  Edge verbindet lokale IT-Infrastrukturen mit Cloud-Services

2.3 Sie erhöhen die Verfügbarkeit Ihrer IT-Systeme

Unternehmen und Behörden, die kritische Infrastrukturen (KRITIS) betreiben, sind auf die ständige Verfügbarkeit ihrer IT-Systeme angewiesen. Zu solchen Unternehmen zählen beispielsweise Energieversorger, Banken oder Firmen aus dem Gesundheitswesen. Im Rahmen der Desaster Recovery arbeiten solche Unternehmen mit redundanten Rechenzentren. Diese sind mit großem räumlichem Abstand so angelegt, dass beide nicht gleichzeitig durch ein überregionales Ereignis wie Hochwasser, Erdbeben oder einen Chemie- und/oder Atomunfall ausfallen [11]. Die Rechenzentren stellen dieselben Serverfunktionen bereit wie die Hauptrechenzentren und dienen zur Entlastung sowie zur Vorbeugung vor Ausfällen.

Die Auslagerung eigener IT-Infrastrukturen in Redundanzrechenzentren bietet z. B. KRITIS-Unternehmen eine einfache Möglichkeit, die Empfehlungen des BSI umzusetzen und sicherzustellen, dass Server, Speicher und Kundendaten auch dann zur Verfügung stehen, wenn es durch Naturgewalten wie Erdbeben oder Hochwasser an einem Ort zu Ausfällen käme [12].

KRITIS-Unternehmen profitieren darüber hinaus finanziell: Aufgrund von Skaleneffekte arbeiten große Rechenzentren sehr kosteneffizient [13], hohe Eigeninvestitionen werden vermieden.

2.4 Sie gewinnen Flexibilität durch Skalierbarkeit

Interne Rechenzentren stehen oft vor einem Dilemma: Entweder sind sie für Belastungsspitzen unzureichend ausgelegt und riskieren Performance-Probleme und Ausfälle, oder sie werden für Belastungsspitzen überdimensioniert und riskieren Überkapazitäten und hohe Folgekosten.

Externe Rechenzentren können dieses Problem lösen, indem sie Kapazitäten dynamisch nach Bedarf bereitstellen. Ob für kurzfristigen Bedarf an Rechenleistung oder kontinuierliches Wachstum – die Auslagerung der IT-Infrastruktur in ein externes Rechenzentrum ermöglicht flexible Skalierung. Damit lassen sich selbst unvorhergesehene Belastungsspitzen auffangen, während im Normalbetrieb nur die tatsächlich benötigten Kapazitäten bezahlt werden.

2.5 Sie gleichen Fachkräftemangel aus

Der Mangel an Fachkräften stellt für IT-Verantwortliche in Deutschland ein großes Problem dar. Laut Umfragen mehrerer IT-Dienstleister sehen die meisten befragten IT-Führungskräfte diesen Engpass an IT-Experten als eine der größten Gefahren für ihr Unternehmen [4, 14]. Etwa die Hälfte der Befragten nennt fehlende Talente, den schnellen technologischen Wandel und die Bindung von Mitarbeitern als zentrale Herausforderungen im Technologiesektor [14]. Besonders mittelständische Unternehmen geraten ohne genügend qualifiziertes Personal unter Druck [4].

Rund drei Viertel der befragten Unternehmen sowie etwa 90 % der CIOs und IT-Leiter sind deshalb überzeugt: Wer seine IT-Infrastruktur an ein externes Rechenzentrum auslagert, kann den Fachkräftemangel ausgleichen [4].

Je nach Anbieter können IT-Kompetenzen aus verschiedenen Bereichen flexibel ergänzt werden, z. B. über zubuchbare Servicepakete. So können Sie gezielt Lücken im eigenen Team schließen. Zudem hilft es, wiederkehrende Aufgaben und den technischen Betrieb in erfahrene Hände zu geben. Das entlastet Ihr eigenes Team und senkt das Risiko von Fehlern.

Fakt

- Der Fachkräftemangel wird als größte Herausforderung für den Betrieb eines eigenen Rechenzentrums bewertet.
- Durch die Auslagerung firmeneigener IT-Infrastrukturen an ein externes Datacenter kann der Fachkräftemangel ausgeglichen werden.
- IT-Expertise kann in Form von Service-Paketen gebucht werden.

2.6 Sie sparen Infrastrukturkosten durch Serverhousing

Der Betrieb eines eigenen Rechenzentrums ist mit vielfältigen Kosten verbunden. Neben den hohen Anfangsinvestitionen für redundante Stromversorgung und Klimatisierung und besonders gesicherte Räumlichkeiten fallen im laufenden Betrieb regelmäßig Ausgaben für Wartung, Energie und Zertifizierungen an. Hinzu kommen Personalkosten sowie zeitlicher und finanzieller Aufwand für Schulungen oder Versicherungen, die etwa bei Brand- oder Einbruchsschäden greifen müssen.

Durch IT-Outsourcing lassen sich viele dieser Aufwände spürbar reduzieren. Schon beim Server-Housing profitieren Sie von einer professionellen Rechenzentrumsinfrastruktur, ohne diese selbst betreiben zu müssen. Ihre eigene Hardware bleibt dabei unter Ihrer Kontrolle, während Sie Ihre Fixkosten reduzieren.

Dies sind Ihre Vorteile im Überblick:

- **Keine eigenen Infrastrukturkosten**
  Investitionen in ein eigenes Rechenzentrumsgebäude, unterbrechungsfreie Stromversorgung, Brandmelde- und Löschtechnik, Zugangssicherheit oder Klimatisierung entfallen. In einem externen Rechenzentrum ist diese Grundausstattung bereits vorhanden.

- **Reduzierte Betriebskosten**
  Die Energieversorgung, Klimatisierung und Netzwerkanbindung werden in einem externen Rechenzentrum effizienter betrieben. Das senkt Ihre laufenden Kosten im Vergleich zu einem Eigenbetrieb deutlich.

- **Reduzierte Aufwände für Gebäude- und Anlagensicherheit**
  Aufwendige Zertifizierungen (z. B. ISO 27001, EN50600), Brandschutzmaßnahmen oder redundante Energieversorgung müssen Sie nicht mehr selbst umsetzen oder warten.

- **Besser Kostenplanbarkeit**
  Während die laufenden Kosten im Eigenbetrieb schwanken können, zahlen Sie in einem externen Rechenzentrum eine fixe monatliche Gebühr für die Nutzung der Services. Zudem können Sie Zusatzservices wie Remote Hands flexibel zubuchen.

- **Skalierbarkeit ohne Investitionsrisiko**
  Ihre Serverkapazitäten können Sie im externen Rechenzentrum bei Bedarf erweitern, ohne selbst in neue Infrastruktur investieren zu müssen.

2.7 Sie verbessern die Nachhaltigkeit Ihres Unternehmens

Ab 2025/2026 bringt das neue Energieeffizienzgesetz (EnEfG) weitreichende Veränderungen für Betreiber von Rechenzentren. Wer ein Rechenzentrum mit einer redundanten Nennanschlussleistung ab 300 kW betreibt, ist dann gesetzlich verpflichtet, Maßnahmen zur Steigerung der Energieeffizienz und zur Senkung des Energieverbrauchs umzusetzen [15, 16]

Dazu gehören unter anderem:

- konkrete Grenzwerte für das Verhältnis von eingespeister zu tatsächlich genutzter Energie [16], der vollständige Umstieg auf erneuerbare Energien ab 2027 [16] ,
- die Umsetzung eines Konzepts zur Wiederverwendung von Abwärme [16] sowie
- die Einführung eines Energie- oder Umweltmanagementsystems bei besonders hohem Energieverbrauch [15, 17].

(eine ausführlichere Beschreibung der Ziele des EnEfG finden Sie unter 3.4)

Für Unternehmen mit einem eigenen Rechenzentrun kann das eine aufwändige Umstellung bedeuten, sowohl technisch als auch organisatorisch. Externe Rechenzentren sind hier oft im Vorteil: Dank standardisierter Prozesse, spezialisierter Fachkräfte und größerer Skaleneffekte können sie die EnEfG-Vorgaben meist schneller, effizienter und nachhaltiger umsetzen.

2.8 Sie profitieren von modernsten Sicherheitskonzepten

Die Sicherheit der eigenen Server ist für Unternehmen von existenzieller Bedeutung. Ein Verlust gespeicherter Daten kann nicht nur hohe finanzielle Schäden verursachen, sondern auch das Vertrauen von Kunden und Partnern nachhaltig schädigen.

Dabei geht es nicht nur um Cyberangriffe. Auch physische Risiken, etwa durch extreme Wetterereignisse, sind für Unternehmen eine große Herausforderung. Hinzu kommt das Risiko zentralisierter Datenhaltung: Sind alle Server an einem Ort untergebracht, steigt die Gefahr eines Totalausfalls erheblich. So befinden sich beispielsweise Serverräume oft im Kellergeschoss – dort, wo sie besonders anfällig für Überschwemmungen durch steigendes Grundwasser, Starkregen oder Schneeschmelze sind. Kommt es zu Schäden an der Hardware, können diese ganze Geschäftsbereiche lahmlegen.

Für viele Unternehmen, insbesondere außerhalb der IT-Branche, ist das Thema IT-Sicherheit schwer greifbar – technisch komplex, aufwendig und kostenintensiv. Schnell stellt sich die Frage: „Sicherheit – ja, aber zu welchem Preis?"

Externe Rechenzentren schaffen hier einen echten Mehrwert. Durch standardisierte Sicherheitskonzepte, den Einsatz modernster Technik und geteilte Infrastrukturkosten bieten sie ein hohes Maß an Sicherheit zu planbaren und im Vergleich geringeren Kosten.

Unternehmen profitieren von:

- physischer Sicherheit (z. B. Zutrittskontrollen, Videoüberwachung),
- modernem Brandschutz,
- umfassendem Datenschutz und
- geprüfter Informationssicherheit.

Ein weiterer Vorteil: Server können dezentral auf mehrere Standorte verteilt werden. Das senkt das Risiko eines gleichzeitigen Ausfalls erheblich. Selbst im Ernstfall, z. B. beim Auftreten eines Naturereignisses, bleiben die Daten durch redundante Speicherung geschützt und verfügbar.

Serversicherheit auf einen Blick

- Für externe Datacenter gehört IT-Sicherheit zum Kerngeschäft – und ist daher professionell.
- Hohe Anforderungen an Gebäudesicherheit und Schutzkonzepte bieten maximale Sicherheit.
- Das dezentrale Serverhousing beugt vollständigen Datenverlusten vor.

3 Anforderungen, die ein externes Datacenter erfüllen muss

Eine moderne Infrastruktur, maximale Kostentransparenz, hohe Skalierbarkeit und zeitgemäße Sicherheitskonzepte zählen zu den größten Vorteilen externer Datacenter. Damit Unternehmen von diesen Mehrwerten auch optimal profitieren, müssen sie bei der Wahl des richtigen Anbieters noch weitere Aspekte berücksichtigen. Dazu gehören insbesondere die geografische Lage, die für die Performance sehr wichtige Anbindung sowie die verfügbaren Zertifizierungen.

3.1 Räumliche Nähe zum Anbieter

Die Auslagerung des kritischen Datenbestands ist Vertrauenssache. Auf der einen Seite lässt sich das erforderliche Vertrauen über Sicherheitsstandards, Datenschutzrichtlinien und andere externe Faktoren aufbauen. Aber das ist nur die eine Seite der Medaille. Denn Vertrauen entsteht am schnellsten zwischen Menschen. Und selbst im digitalen Zeitalter hat der persönliche Kontakt noch immer oberste Priorität. Wer sein Gegenüber kennt, ihm – ohne zwischengeschalteten Bildschirm – einmal in die Augen geschaut und das Besprochene per Handschlag besiegelt hat, geht in der Regel mit einem besseren Gefühl nach Hause. Gleiches gilt für eventuelle Unstimmigkeiten oder Unsicherheiten. Wenn der Vertragspartner in der Nähe ist, erleichtert das die gesamte Kommunikation.

3.2 Serverhousing in Deutschland

Wo werden Ihre Server genau gelagert? Housing vor Ort – also in Deutschland – basiert auf Vertrauen in hiesige Anbieter. Aber es ist vor allem auch ein Sicherheitsaspekt. Wichtig für die Sicherheit der Server und den Datenschutz ist, dass deutsches bzw. europäisches Recht greift. Behörden können nur bei berechtigtem Interesse, z. B. bei Strafverfolgung, Auskunftsrecht erhalten[18]. Ganz anders sieht es zum Beispiel in den USA aus: Die NSA, die National Security Agency, kann amerikanische Unternehmen jederzeit und ohne Einschränkungen zur Datenherausgabe auffordern und die Unternehmen müssen Folge leisten[19]. Dieses Behördenrecht gilt auch, wenn der entsprechende Server von einem amerikanischen Unternehmen außerhalb der USA betrieben wird[19, 20]. Folglich sollte das Rechenzentrum seinen Unternehmenssitz sowie seinen Serverstandort innerhalb Deutschlands haben. Nur so ist maximale Sicherheit gewährleistet.

3.3 Schnelle Anbindung

Für eine konstant hohe Performance müssen die Server in einem Rechenzentrum zum einen untereinander optimal verbunden sein. Zum anderen bedarf es einer bestmöglichen Anbindung des externen Rechenzentrums an das Kundenunternehmen bzw. Uplinks zu einer Vielzahl von Providern. Hierzu sind einige Voraussetzungen erforderlich und es gibt diverse Möglichkeiten, für optimale Performance und Stabilität zu sorgen. Zu den Voraussetzungen gehört eine Anbindung des Kunden an das Datacenter bzw. Internet mit großer Bandbreite. Wie gut die Anbindung in der Praxis jeweils ist, lässt sich beispielsweise bei Videokonferenzen prüfen: Sind Bild und Ton klar? Für eine optimale Anbindung sorgen in der Regel Glasfaserkabel, die Daten per Lichtwelle übertragen. Genau hier liegt einer der großen Vorteile der Datenauslagerung. Ein externes Rechenzentrum bietet Ihnen genau diejenige Anbindung, die Sie für Ihr Unternehmen mit seinen spezifischen Rahmenbedingungen benötigen – und zwar hoch performant und ausfallsicher. Im eigenen Serverraum ist das in der Regel nicht leistbar.

Performante Anbindung an externe Rechenzentren auf einem Blick

- **Glasfaserkabel** sorgen für optimale Performanz und Hochverfügbarkeit.
- **Redundante Standleitungen** sichern die Überlasten und die Ausfälle der Standard-Anbindung ab.
- **Technologien** wie MPLS (Multiprotocol Label Switching), SD WAN (Software-Defined Wide Area Network), Peering, autonome Systeme (AS) oder Cloud-Connect sichern die Qualität der Anbindung je nach Bedarf individuell ab.

3.4 Ziele des neuen Energieeffizienzgesetz (EnEfG)

Ab 2025/2026 stellt das neue Energieeffizienzgesetz (EnEfG) klare Anforderungen an Betreiber von Rechenzentren. Ziel ist es, den Energieverbrauch spürbar zu senken und die Energieeffizienz langfristig zu verbessern.

Konkret verlangt das Gesetz die Umsetzung geeigneter Maßnahmen, etwa die Nutzung erneuerbarer Energien für die Stromversorgung oder die Einspeisung von Abwärme in bestehende Wärmenetze.

Rechenzentren mit einer redundanten Nennanschlussleistung ab 300 kW müssen die folgenden Vorgaben umsetzen [15, 16]:

- Für neu in Betrieb genommene Rechenzentren gilt ab dem 01.07.2026 eine Energieverbrauchseffektivität (auch: PUE (Power Usage Effectiveness) -Wert) von maximal 1,2 [16]. Der PUE-Wert ergibt sich aus der eingespeisten Energiemenge, geteilt durch die verbrauchte Energiemenge – je näher das Ergebnis an 1,0 liegt, desto effizienter arbeitet ein Rechenzentrum.
- Bestehende Rechenzentren, die vor dem 1.7.2026 in Betrieb genommen wurden, müssen ab dem 1.7.2027 einen PUE-Wert von höchstens 1,5 nachweisen. Ab dem 1.7.2030 gilt ein Wert von maximal 1,3 im Jahresdurchschnitt [16].
- Ab 1.1.2024 müssen mindestens 50 % des Stromverbrauchs eines Rechenzentrums aus erneuerbaren Energien stammen [16].
- Ab 1.1.2027 sollen 100 % des Stromverbrauchs aus erneuerbaren Energien stammen [16].
- Rechenzentren die ab dem 1.7.2026 in Betrieb gehen, müssen mindestens 10 % der anfallenden Energie wiederverwenden, beispielsweise in Form von Abwärme. Ab dem 1.7.2027 müssen sie 15 %, und ab dem 1.7.2028 mindestens 20 % der anfallenden Energie wiederverwenden [16].
- Bis zum 1.7.2025 ist zudem ein Energie- oder Umweltmanagementsystem einzurichten [15], wenn der jährliche durchschnittliche Gesamtendenergieverbrauch 7,5 GWh übersteigt [17].

Für Unternehmen mit eigenen Rechenzentren bedeuten diese Vorgaben möglicherweise erhebliche technische, strukturelle und finanzielle Herausforderungen. Externe Rechenzentren hingegen ermöglichen durch ihre Skaleneffekte, professionellen Strukturen und spezialisierten Teams eine effizientere und kostengünstigere Umsetzung entsprechender Maßnahmen. Durch die Auslagerung eigener IT-Infrastrukturen in ein geeignetes Rechenzentrum können Sie den Zielvorgaben des EnEfG deshalb schneller und nachhaltiger gerecht werden.

3.5 Spezielle Anforderungen des BSI an kritische Infrastrukturen (KRITIS)

Das Bundesamt für Sicherheit in der Informationstechnik stellt bestimmte Anforderungen an Unternehmen und Institutionen, deren Ausfall oder Beeinträchtigung massive Auswirkungen auf die Gesellschaft hätte. Zu diesen KRITIS zählen Unternehmen aus den Bereichen Energie, Wasser, Gesundheit, Informationstechnik und Telekommunikation [21].

Rechenzentren zählen ebenfalls zu den KRITIS-Unternehmen, wenn sie eine IT-Leistung von 3,5 MW überschreiten [22]. Diese Rechenzentren unterliegen dann speziellen gesetzlichen Anforderungen, zu deren Erfüllung verschiedene Maßnahmen implementiert werden müssen [23]. Dazu zählen unter anderem Maßnahmen in den folgenden Bereichen:

- **Informationssicherheitsmanagements:**
  Einführung eines ISMS sowie Vorgaben zu Risikobewertung, Maßnahmenableitung und Asset-Management
- **technische und organisatorische Sicherheit:**
  Schutzmaßnahmen gegen Schadprogramme, Datensicherung, Schwachstellenmanagement sowie klare Regelungen für Zugriffs- und Benutzerrechte
- **physische und personelle Sicherheit:**
  Zutrittskontrollen, Videoüberwachung sowie Sicherheitsüberprüfungen und Rollenkonzepte für Mitarbeitende
- **Gewährleistung** der Betriebskontinuität und Überwachung: Notfallpläne, interne und externe Prüfungen, Log-Analysen und Penetrationstests
- **Lieferanten- und Vorfallmanagement:**
  Vorgaben für Dritte sowie strukturierte Prozesse zur Erkennung und Bearbeitung von Sicherheitsvorfällen.

Darüber hinaus sind Betreiber von KRITIS verpflichtet, erhebliche IT-Sicherheitsvorfälle unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden [23].

Die Umsetzung der Maßnahmen müssen Betreiber von KRITIS dem BSI alle zwei Jahre durch §8a BSIG-Prüfungen nachweisen. Diese Prüfungen werden ausschließlich von speziellen Prüfteams durchgeführt. Eine spezifische Zertifizierung durch die Prüfer oder das BSI gibt es nicht.

Durch den Nachweis der Zertifizierung nach DIN EN 50600 (physische Sicherheit von Rechenzentren) und der Zertifizierung nach ISO/IEC 27001 (Informationssicherheitsmanagement) erhalten Sie aber einen Hinweis darauf, ob das jeweilige Rechenzentrum dem Stand der Technik entspricht.

3.6 Anforderungen durch NIS2

Die EU NIS-2-Richtlinie soll die Cybersicherheit der Netz- und Informationssysteme und das Sicherheitsniveau aller EU-Mitgliedsstaaten erhöhen und harmonisieren.

Die Anforderungen der EU NIS-2-Richtlinie werden in Deutschland durch das deutsche „Gesetz zur Umsetzung der NIS-2-Richtlinie" implementiert. Dieses Gesetz liegt derzeit als Referentenentwurf vor und unterscheidet zwischen verschiedenen Kategorien von Einrichtungen:

- „Wichtige Einrichtungen"
  (z. B. mittelgroße Unternehmen)
- „Besonders wichtige Einrichtungen"
  (z. B. größere oder systemrelevante Unternehmen)
- Betreiber kritischer Anlagen
  (KRITIS; Unternehmen, die kritische Dienstleistungen erbringen)[24].

3.6.1 Bedeutung für Rechenzentren

Das Gesetz zur Umsetzung der NIS-2-Richtlinie klassifiziert „Anbieter von Rechenzentrumsdiensten" als „besonders wichtige Einrichtungen" im Sektor „Digitale Infrastruktur"[24]. Rechenzentren, die unter die NIS-2-Regelung fallen, müssen ein strukturiertes IT-Risikomanagement einführen und technische wie organisatorische Schutzmaßnahmen umsetzen, unter anderem zur Vorfallbewältigung,

Lieferkettensicherheit, Zugriffskontrolle oder Schwachstellenmanagement (§ 30). Die Maßnahmen müssen dem Stand der Technik entsprechen und dokumentiert werden.

Bei erheblichen Sicherheitsvorfällen gilt eine Meldepflicht (§ 30): Innerhalb von 24 Stunden ist eine Erstmeldung, nach spätestens 72 Stunden eine vertiefte Meldung und innerhalb eines Monats ein Abschlussbericht einzureichen. Zusätzlich sind Rechenzentrumsbetreiber verpflichtet, sich beim Bundesamt zu registrieren und alle drei Jahre den Nachweis über die Umsetzung der Sicherheitsanforderungen zu erbringen (§§ 33, 39).

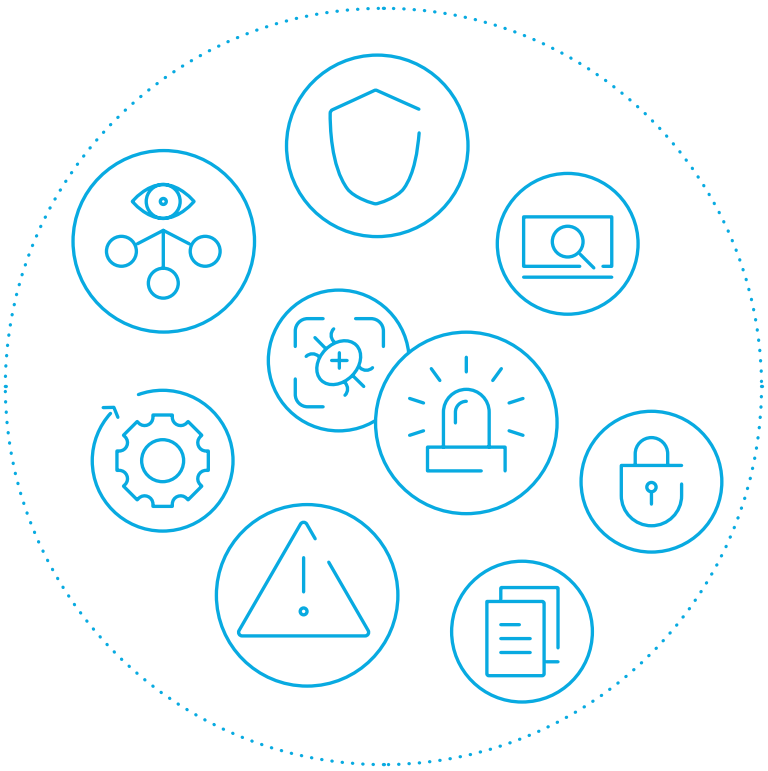
Die Geschäftsleitung trägt die Verantwortung für die Umsetzung, muss regelmäßig geschult werden und kann bei Pflichtverstößen haftbar gemacht werden (§§ 38). Zudem kann vorgeschrieben werden, dass nur zertifizierte IT-Produkte oder -Dienste eingesetzt werden dürfen (§ 30 Abs. 6)[24].

3.6.2 Bedeutung für KRITIS-Betreiber

KRITIS-Betreiber unterliegen zusätzlich zu den allgemeinen NIS-2-Pflichten weitergehenden Anforderungen. Sie müssen ein besonders hohes Schutzniveau sicherstellen – auch über Standardmaßnahmen hinaus, sofern dies angesichts des Risikos verhältnismäßig ist (§ 31 Abs. 1).

Zentral ist die Pflicht zum Einsatz von Systemen zur Angriffserkennung, die laufend Bedrohungen analysieren und auf Sicherheitsvorfälle reagieren (§ 31 Abs. 2). Bei Meldungen müssen sie zusätzlich angeben, welche Anlage und kritische Dienstleistung betroffen ist (§ 32 Abs. 3).

Darüber hinaus gilt eine erweiterte Nachweispflicht gegenüber dem Bundesamt: Sicherheitsmängel sind offenzulegen, zu beheben und nachzuverfolgen (§ 39). Der Einsatz kritischer IT-Komponenten ist anzeigepflichtig und kann untersagt werden, wenn sicherheitspolitische Risiken bestehen. Nur vertrauenswürdige Hersteller sind zulässig (§ 41)[24].



Grafik: Übersicht der Sicherheitsmaßnahmen und Anforderungen für KRITIS-Betreiber gemäß NIS-2-Richtlinie. Diese Maßnahmen umfassen Angriffserkennung, kontinuierliche Bedrohungsanalyse und die Sicherstellung eines hohen Schutzniveaus.

3.6.3 Die Anforderungen im Vergleich

Pflichten durch das deutsche Gesetz zur Umsetzung der NIS-2-Richtlinie [24]	Pflichten für Rechenzentren (allgemein)	Pflichten zusätzlich für KRITIS-Betreiber
IT-Risikomanagement	Pflicht nach Stand der Technik (§ 30)	muss besonders hohes Schutzniveau erreichen (§ 31 Abs. 1)
Vorfallmeldungen	24h-/72h-/1-Monats-Fristen (§ 32 Abs. 1)	zusätzlich Angaben zur betroffenen Anlage und Dienstleistung (§ 32 Abs. 3)
Registrierung und Nachweis	Registrierung innerhalb von 3 Monaten (§ 33 Abs. 1); Hinweise zum Nachweis nicht explizit enthalten	Registrierung innerhalb von 3 Monaten (§ 33 Abs. 1) + 3-jährlicher Nachweis (§ 39 Abs. 1) + behördliche Nachverfolgung (§ 39 Abs. 2)
Angriffserkennung	empfohlen oder implizit enthalten	verpflichtend, kontinuierlich, automatisiert + müssen sowohl präventiv wirken als auch Störungen erkennen und eingrenzen (§ 31 Abs. 2)
Verantwortung der Geschäftsleitung	Umsetzungs- und Schulungspflicht (§ 38)	
Produkte und Komponenten	ggf. EU-zertifizierte IT-Produkte verpflichtend (§ 30 Abs. 6)	zusätzlich Anzeige- und Untersagungspflichten bei kritischen Komponenten (§ 41)

Für alle Rechenzentren, die unter die NIS-2-Kategorie „wichtige Einrichtung" oder „besonders wichtige Einrichtung" fallen, gelten umfassende Anforderungen an Informationssicherheit, Risikomanagement und Meldepflichten.

Für KRITIS-Betreiber verschärfen sich diese Vorgaben deutlich: Sie müssen weitereichende technische Maßnahmen umsetzen, Systeme zur Angriffserkennung verpflichtend betreiben, zusätzliche Nachweise erbringen und dürfen sicherheitskritische Komponenten nur unter bestimmten Voraussetzungen verwenden.

Die Einhaltung dieser Anforderungen erfordert nicht nur technisches Know-how, sondern auch strukturelle und prozessuale Reife. Beides macht die Zusammenarbeit mit spezialisierten Rechenzentrumsanbietern zu einer strategisch sinnvollen Option.

3.7 Zertifizierte Sicherheitskonzepte

Rechenzentren gleichen einem Hochsicherheitstrakt. Für den Betrieb müssen sie diverse Auflagen auf verschiedenen Ebenen erfüllen. Angefangen bei der Standortwahl über die Architektur und die Gebäudeabsicherung bis hin zu Zutrittskontrollen gibt es zahlreiche Faktoren, die im Zusammenspiel maximale Sicherheit bieten. Die Security-Maßnahmen zielen auf die Vorbeugung und Abwehr interner und externer Zugriffe sowie auf die Minimierung möglicher Gefahren durch Naturkatastrophen oder terroristische Angriffe. Einen entsprechenden Grundschutzkatalog hat das Bundesamt für Sicherheit in der Informationstechnik herausgegeben. Ob und inwieweit sich die Betreiber von Rechenzentren an diese Vorgaben halten, können sie mithilfe von Zertifizierungen nachweisen. Vor allem die Standards des Deutschen Instituts für Normung geben in Form der weithin bekannten DIN-Normen Auskunft über die Einhaltung der Regelwerke. Das europäische Pendant sind die EN-Normen. International gültige Standards spiegeln sich in den ISO-Normen wider. Eine entsprechende Zertifizierung ist für Rechenzentren nicht zwingend vorgeschrieben. Wer den Zertifizierungsprozess aber freiwillig und erfolgreich absolviert hat, steht für einen hohen Selbstanspruch bezüglich der Umsetzung geltenden Rechts und hoher Qualitäts-, Prozess- und Sicherheitsvorgaben.

Relevant für externe Datacenter sind insbesondere:

- **DIN EN 50600**
  fokussiert auf die physische Sicherheit von Rechenzentren.

- **ISO 50001**
  bildet die Grundlage für ein standardisiertes Energiemanagementsystem, das auf eine fortlaufende Verbesserung der Energieeffizienz abzielt.

- **ISO/IEC 27001**
  bewertet das Informationssicherheitsmanagement im Rechenzentrum.

- **ISO 9001**
  zertifiziert das Qualitätsmanagement des Rechenzentrumbetreibers.

- **TÜViT TSI.STANDARD V4.3 Level 3 (erweitert)**
  zertifiziert Verfügbarkeit und Sicherheit auf Level 3 (hoher Schutzbedarf)

Mindestens eines, besser zwei der genannten Zertifikate bürgen für höchste Sicherheitsstandards. Durchgeführt werden die dafür erforderlichen Audits zum Beispiel vom TÜV.

4 Direkt anwenden: Checklisten für eine erfolgreiche Dienstleistersuche

Die Suche nach dem richtigen Partner für Ihre sensiblen Unternehmensdaten kann aufgrund der Angebotsfülle sehr ressourcenintensiv sein. Hinzu kommen Unsicherheiten bezüglich der Anforderungen und des Leistungsspektrums. Damit Ihre Recherche nach einem geeigneten Partner schnell und zuverlässig zum Erfolg führt, können Sie sich an den folgenden Checklisten orientieren. Sie enthalten die wichtigsten Kriterien, auf die Sie bei der Dienstleisterauswahl unbedingt achten sollten. Bitte berücksichtigen Sie, dass diese Checklisten keinen Anspruch auf Vollständigkeit haben. Gerade unternehmensspezifische Anforderungen sind jeweils individuell zu überprüfen.

4.1 Mit den folgenden Kriterien sichern Datacenter eine bestmögliche Internetanbindung

IT-Systemausfälle verursachen in Deutschland jährlich Schäden in Milliardenhöhe. Laut Bitkom beliefen sich die Schäden durch IT- und Produktionsausfälle 2024 auf rund 54,5 Milliarden Euro[25]. Unternehmen sind heute auf den ständigen Zugriff auf ihre Daten und Systeme angewiesen. Können Firmen nicht auf ihre Daten zugreifen, kommt das gesamte Geschäft zum Erliegen. In Zeiten digitaler Transformation, mobilen Arbeitens und mobiler Kommunikation in Echtzeit gehört die permanente Verfügbarkeit zur wichtigsten Voraussetzung für die Wettbewerbsfähigkeit. Sichere und hochleistungsfähige Glasfaser- und Internetanbindungen sind daher ein entscheidender Aspekt und Gradmesser für die Qualität eines Datacenters.

Checkliste: Mit den folgenden Kriterien sichern Datacenter eine bestmögliche IP-/Internetanbindung.	**Ja?**	**Nein?**
IP-/Internet-Anbindung		
Redundante Anbindung		
Next Generation Network (NGN) auf Basis eines Carrier-Ethernet-Systems		
Cat6-/Cat7-Verbindungen		
Internet-Konnektivität ab 1 Gbit/s		
IP-v4- bzw. IP-v6-Netze		
Meet-Me-Anbindung		
Direkte Anbindung an den Internetknoten Frankfurt am Main (DE-CIX)		

4.2 So garantiert ein professionelles Datacenter eine optimale Stromversorgung

Für IT-Systeme führen selbst minimale Stromausfälle zu erheblichen Störungen. Eine optimale, unterbrechungs- und störungsfreie Stromversorgung hat bei der Auswahl eines Datacenters daher oberste Priorität.

4.3 Diese Sicherheitsmaßnahmen sollte ein gutes Datacenter bieten

IT-Ausfälle sind nicht immer nur die Folge von Ransomware-Angriffen. Mitte 2024 verursachte ein fehlerhaftes Update einer Cybersicherheitslösung von CrowdStrike IT-Ausfälle bei 331 Unternehmen in Deutschland (26). Fast die Hälfte der betroffenen Unternehmen mussten dabei ihre Arbeit für durchschnittlich zehn Stunden einstellen (26). Aber nicht nur ein längerer Komplettausfall, sondern bereits einfache Spannungsschwankungen oder Kurzausfälle im Stromnetz können reichen, um Hard- oder Software zu schädigen oder so zu stören, dass schwere Fehler in den IT-Prozessen auftreten. Um solche Worst-Case-Szenarien vollends ausschließen zu können, sollten professionelle Datacenter nicht nur physisch abgesichert, sondern auch mit umfassenden IT-Sicherheitsmaßnahmen ausgestattet sein.

5 Fazit

Zunehmender Fachkräftemangel, steigender Kostendruck und eine sich stetig ändernde IT-Landschaft sorgen dafür, dass Outsourcing weiter an Bedeutung gewinnen wird. Immer mehr Unternehmen verlagern ihre IT in externe Rechenzentren oder die Cloud. 89 % der Unternehmen in Deutschland nutzen inzwischen Cloud-Services.

Auch Colocation-Angebote gewinnen an Bedeutung[2]. Immer weniger Unternehmen planen intern[3]. Noch in diesem Jahr könnten bis zu 80 % der bislang firmeneigenen Rechenzentren ausgelagert werden[3, 5]. Die Vorteile sprechen für sich: einfache Skalierbarkeit, hohe Sicherheitsstandards, Kosteneffizienz, Entlastung des eigenen IT-Personals[6].

Durch diese Vorteile werden Unternehmen agiler und widerstandsfähiger.

Eine hohe Performance, stabile Verfügbarkeit sowie maximale Daten- und IT-Security entscheiden dann darüber, wer im globalen Wettstreit die Nase vorn haben wird. Ein kompetenter IT-Dienstleister ist dann der beste Partner für eine sichere digitale Zukunft.

Ihr Experten-Kontakt

Sandra Warg
Produktmanager Datacenter & Infrastruktur
E-Mail: sandra.warg@enviaTEL.de

6 Literaturverzeichnis

1 **Bitkom e.V.; Hintemann; Hinterholzer; Progni .** Rechenzentren in Deutschland. Aktuelle Marktentwicklung - Stand 2024. [Online] 2024. [Zitat vom: 06. 03 2025.] https://www.bitkom.org/sites/main/files/2024-11/241121-studie-rechenzentrumsmarkt.pdf#:~:text=Anschlussleistungen%20im%20zwei,Angebote.

2 **Borderstep Institut; Bitkom, Digitalverband.** Rechenzentren: Borderstep erstellt Studie für Bitkom. [Online] 2023. [Zitat vom: 06. 03 2025.] https://www.borderstep.de/2023/05/25/rechenzentren-borderstep-erstellt-studie-fuer-bitkom/#:~:text=In%20Deutschland%20wird%20das%20Wachstum,gibt%20es%20in%20Deutschland%20derzeit.

3 **Vertikal.de.** IT-Outsourcing & Fachkräftemangel: Das Ende der firmeneigenen Rechenzentren rückt näher. [Online] 2022. [Zitat vom: 06. 03 2025.] https://www.vertical.de/artikel/it-outsourcing-fachkraeftemangel-das-ende-der-firmeneigenen-rechenzentren-rueckt-naeher/#:~:text=Das%20Marktforschungsunternehmen%20Gartner%20liefert%20die,blockiert%20diese%20nun%20veraltete%20Vorgehensweise.

4 **IT-Markt; Netzmedien AG.** Umfrage von Technogroup. Fachkräftemangel erfasst Rechenzentren. [Online] 2023. [Zitat vom: 06. 03 2025.] https://www.it-markt.ch/news/2023-05-22/fachkraeftemangel-erfasst-rechenzentren#:~:text=.

5 **Gartner, Inc.** The Data Center Is (Almost) Dead. [Online] 2019. [Zitat vom: 06. 03 2025.] https://www.gartner.com/smarterwithgartner/the-data-center-is-almost-dead.

6 **International Data Corporation (IDC); Datacenter One GmbH.** Die Nachfrage nach Colocation und Edge Computing steigt weiter an. Ergebnisse einer IDC-Studie in Partnerschaft mit Datacenter One. [Online] 2022. [Zitat vom: 06. 03 2025.] https://www.dc1.com/news/2022/12/05/die-nachfrage-nach-colocation-und-edge-computing-steigt-weiter-an/.

7 **EDGEIR.com Industry Review.** Edge computing to face a paradigm shift as worldwide spend is set to exceed $232 billion. [Online] 20. 05 2024. [Zitat vom: 06. 03 2025.] https://www.edgeir.com/edge-computing-to-face-a-paradigm-shift-as-worldwide-spend-is-set-to-exceed-232-billion-20240320#:~:text=Worldwide%20spending%20on%20edge%20computing,Worldwide%20Edge%20Spending%20Guide.

8 **VMware; Khan Asif Azad.** Edge Computing and Industry 4.0. [Online] 29. 10 2024. [Zitat vom: 06. 03 2025.] https://blogs.vmware.com/sase/2024/10/29/edge-computing-and-industry-4-0/#:~:text=Edge%20can%20be%20categorized%20as,the%20importance%20of%20edge%20strategy.

9 Bundesamt für Sicherheit in der Informationstechnik. Sichere Nutzung von EdgeComputing. [Online] 23. 12 2023. [Zitat vom: 06. 03 2025.] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_148.pdf?__blob=publicationFile&v=3.

10 **envia TEL; Sandra Warg.** Edge Computing als vielversprechendes Bindeglied für Cloud-Services. [Online] 21. 01 2022. [Zitat vom: 06. 03 2025.] https://www.enviatel.de/blog/blog/2022/01/21/edge-computing-bindeglied-fuer-cloud-services.

11 **Bundesamt für Sicherheit in der Informationstechnik.** Kriterien für die Standortwahl von. RZ-Standortkriterien. [Online] 12 2024. [Zitat vom: 06. 03 2025.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/RZ-Sicherheit/Standort-Kriterien_Rechenzentren.pdf?__blob=publicationFile&v=5.

12 **eco - Association of the Internet Industry.** DCES: 3 Questions for Sandra Warg, envia TEL GmbH. [Online] 26. 03 2024. [Zitat vom: 06. 03 2025.] https://international.eco.de/news/dces-3-questions-for-sandra-warg-envia-tel-gmbh/#:~:text=It%20is%20no%20coincidence%20that,provision%20of%20the%20required%20services.

13 **Datacenter One GmbH.** Die Nachfrage nach Colocation und Edge Computing steigt weiter an. [Online] 05. 12 2022. [Zitat vom: 06. 03 2025.] https://www.dc1.com/news/2022/12/05/die-nachfrage-nach-colocation-und-edge-computing-steigt-weiter-an/#:~:text=Bewegung%20ist%20beispielsweise%20in%20den,werden%20die%20Rechenkapazit%C3%A4ten%20dorthin%20verlagert.

14 **Equnix.** Fachkräftemangel verlangsamt die Einführung neuer Technologien in deutschen Unternehmen. [Online] 2023. [Zitat vom: 06. 03 2025.] https://www.equinix.de/newsroom/press-releases/2023/08/fachkr-ftemangel-verlangsamt-die-einfhrung-neuer-technologien-in-deutschen-unternehmen.

15 **Bundesamt für Justiz.** Gesetz zur Steigerung der Energieeffizienz in Deutschland1 (Energieeffizienzgesetz - EnEfG). Abschnitt 4 - Energieeffizienz in Rechenzentren / § 12 Energie- und Umweltmanagementsysteme in Rechenzentren. [Online] 13. 11 2023. [Zitat vom: 06. 03 2025.] https://www.gesetze-im-internet.de/enefg/BJNR1350B0023.html/#:~:text=Unbeschadet%20von%20§8%20sind%20Betreiber%20,Umweltmanagementsystem%20einzurichten%20.

16 —. Gesetz zur Steigerung der Energieeffizienz in Deutschland1 (Energieeffizienzgesetz - EnEfG). Abschnitt 4 - Energieeffizienz in Rechenzentren / § 11 Klimaneutrale Rechenzentren. [Online] 23. 11 2023. [Zitat vom: 06. 03 2025.] https://www.gesetze-im-internet.de/enefg/BJNR1350B0023.html.

17 **Justiz, Bundesamt für.** Gesetz zur Steigerung der Energieeffizienz in Deutschland1 (Energieeffizienzgesetz - EnEfG). Abschnitt 3 Energie- oder Umweltmanagementsysteme und Umsetzungspläne für Unternehmen / §8 Einrichtung von Energie- oder Umweltmanagementsystemen. [Online] 13. 11 2023. [Zitat vom: 16. 04 2025.] https://www.gesetze-im-internet.de/enefg/BJNR1350B0023.html/#:~:text=Unternehmen%20mit%20einem%20jährlichen%20durchschnittlichen%20,Satz%201%20oder%20Satz%202%20einzurichten%20.

18 **activeMind.AG.** Datenschutzkonformer Umgang mit Auskunftsersuchen von Polizei und Staatsanwaltschaft. [Online] 13. 07 2019. [Zitat vom: 24. 04 2025.] https://www.activemind.de/magazin/auskunftsersuchen/#:~:text=In%20Erw%C3%A4gungsgrund%2050%20rechtfertigt%20die,als%20berechtigtes%20Interesse%20des%20Verantwortlichen.

19 **Cloudcomputing Insider**; Götz Piwinger. Patriot Act & Co. konterkarieren EU-Rechtsprechung. [Online] 12. 10 2015. [Zitat vom: 24. 04 2025.] https://www.cloudcomputing-insider.de/patriot-act-amp-co-konterkarieren-eu-rechtsprechung-a-507727/#:~:text=Bereitstellung%20geeigneter%20Instrumente%2C%20um%20den,Spionage.

20 **Conceptboard.** Der US Cloud Act: Die Bedrohung des europäischen Datenschutzes. [Online] 2024. [Zitat vom: 24. 04 2025.] https://conceptboard.com/de/blog/us-cloud-act-europaeischer-datenschutz/#:~:text=Die%20Antwort%20lautet%3A%20Ja%2C%20da,eindeutigen%20Widerspruch%20zu%20unserer%20DSGVO.

21 **Bundesamt für Sicherheit in der Informationtechnik.** Was sind Kritische Infrastrukturen? [Online] [Zitat vom: 06. 03 2025.] https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html.

22 **Bundesamt für Sicherheit in der Informationstechnik.** Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV); Anhang 4 (zu § 1 Nummer 4 und 5, § 5 Absatz 4 Nummer 1 und 2); Anlagenkategorien und Schwellenwerte im Sektor Informationstechnik und Telekommun. Teil 3 - Anlagenkategorien und Schwellenwerte. [Online] [Zitat vom: 06. 03 2024.] https://www.gesetze-im-internet.de/bsi-kritisv/anhang_4.html.

23 —. Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 und Absatz 1a BSIG umzusetzenden Maßnahmen. Hinweise zur Umsetzung der Kriterien des § 8a (1) und (1a) BSIG für die Beurteilung der Informationssicherheit bei Betreibern Kritischer Infrastrukturen. [Online] [Zitat vom: 06. 03 2025.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Konkretisierung_Anforderungen_Massnahmen_KRITIS.pdf?__blob=publicationFile&v=18.

24 **Bundesministeriums des Innern.** Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Referentenentwurf des Bundesministeriums des Innern. [Online] 23. 06 2025. [Zitat vom: 14. 07 2025.] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-RefE_2025.pdf?__blob=publicationFile&v=8.

25 **Bitkom, Ralf Wintergerst.** Wirtschaftsschutz 2024. [Online] 28. 08 2024. [Zitat vom: 24. 04 2025.] https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf#:~:text=Ausfall%2C%20Diebstahl%20oder%20Sch%C3%A4digung%20von,vor%20Anmeldung%2014%2C8%2010%2C4%2018%2C8.

26 **Bitkom e.V.** CrowdStrike: Welche Folgen der IT-Ausfall für deutsche Unternehmen hatte. Gemeinsame Presseinformation von Bitkom und BSI. [Online] 19. 09 2024. [Zitat vom: 24. 04 2025.] https://www.bitkom.org/Presse/Presseinformation/CrowdStrike-Folgen-fuer-Unternehmen/#:~:text=Gestrichene%20Flüge%20ausgefallene%20Server%20,nicht%20vollständig%20verhindern%20.

27 **International Data Corporation (IDC).** Data Centers and Our Climate. [Online] 23. 09 2024. [Zitat vom: 06. 03 2025.] https://blogs.idc.com/2024/09/23/data-centers-and-our-climate/#:~:text=poses%20a%20significant%20struggle%20as,growing%20to%20857TWh%20by%202028.

28 **Borderstep Institut; Bitkom e.V.** Rechenzentren: Deutschland verliert den Anschluss. [Online] 2024. [Zitat vom: 06. 03 2025.] https://www.borderstep.de/2024/11/21/rechenzentren-deutschland-verliert-den-anschluss/#:~:text=Traditionelle%20Rechenzentren%20werden%20,mittlerweile%20sichtbarem%20Abwärtstrend%20.

29 **Telecom Review Americas.** Data Centers Face Challenges in the AI Era. [Online] 20. 05 2024. [Zitat vom: 06. 03 2025.] https://www.telecomreviewamericas.com/articles/reports-and-coverage/data-centers-face-challenges-in-the-ai-era/#:~:text=%E2%80%9CMost%20of%20the%20AI%20workloads,Infrastructure%20by%20S%26P%20Global.

30 germandatacenters.com. Data Center Impact Report Deutschland 2024. [Online] 2024. [Zitat vom: 06. 03 2025.] https://www.germandatacenters.com/dcird-24/#:~:text=So%20nimmt%20die%20Branche%20eine,Nachhaltigkeit%20in%20der%20Technologiebranche%20unterstreicht.

31 **Cisco Systems.** Cisco-Studie: Nur 2 % der deutschen Firmen sind auf aktuelle Cyberbedrohungen bestmöglich vorbereitet. Press Release. [Online] 03. 04 2024. [Zitat vom: 06. 03 2025.] https://news-blogs.cisco.com/emea/de/2024/04/03/cisco-studie-nur-2-der-deutschen-firmen-sind-auf-aktuelle-cyberbedrohungen-bestmoeglich-vorbereitet/.

32 **OpenKRITIS.** NIS2 Umsetzungsgesetz. [Online] 2024. [Zitat vom: 06. 03 2025.] https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html.

33 —. NIS2 Umsetzungsgesetz. Fokus: Pflichten von Betreibern und Einrichtungen. [Online] [Zitat vom: 06. 03 2025.] https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html#:~:text=Die%20Anforderungen%20an%20Betreiber%20und,teils%20versch%C3%A4rft%20und%20neu%20strukturiert.

34 —. NIS2 Umsetzungsgesetz. Fokus: Maßnahmen. [Online] [Zitat vom: 06. 03 2025.] https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html#:~:text=Management%20,Maßnahmen%20und%20SzA.

35 —. NIS2 Umsetzungsgesetz; Fokus: Nachweise und Prüfungen. [Online] 2024. [Zitat vom: 06. 03 2025.] https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html#:~:text=,Nachweise%20und%20Prüfungen%20,diese%20Nachweis-Prüfungen%20festlegen%20.

Bei Fragen sind wir gern für Sie da.

Kostenfreie Servicenummer
0800 0 101600
info@enviaTEL.de
enviaTEL.de
envia TEL GmbH
Friedrich-Ebert-Str. 26
04416 Markkleeberg