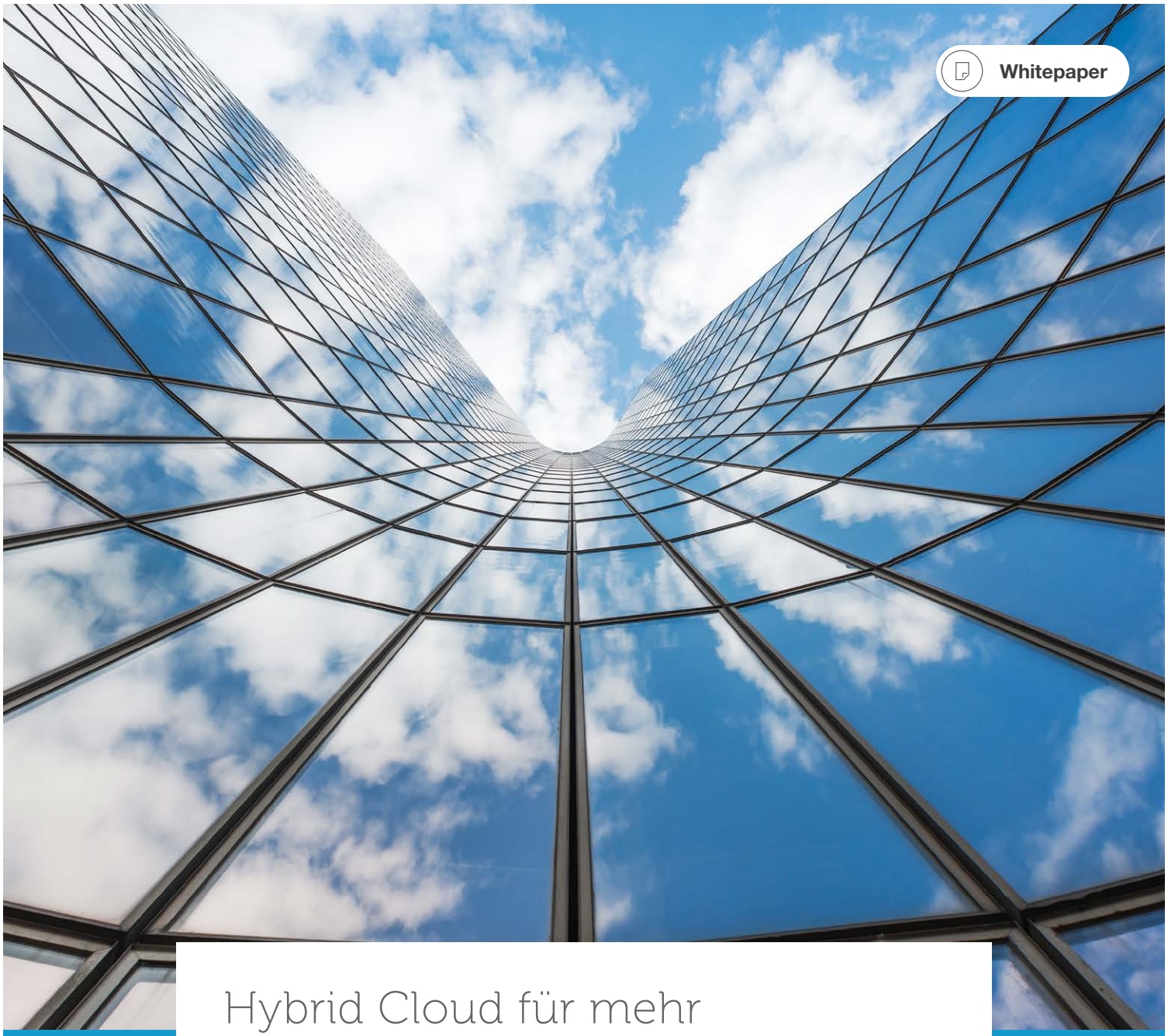
interxion™



Whitepaper

Hybrid Cloud für mehr physische Sicherheit

Interxion Cloud Connect bietet Unternehmen die sicherste und robusteste Hybrid-Cloud-Lösung.

In diesem Whitepaper erläutern wir, wie Unternehmen mit Interxion Cloud Connect von der sichersten und robustesten Hybrid-Cloud-Lösung profitieren können. Durch das Zusammenspiel von solider physischer Sicherheit, Wartung und Support rund um die Uhr, sowie mehr als genug Redundanz für unerwartete Ereignisse, helfen die Colocation-Rechenzentren von Interxion Unternehmen das volle Potenzial der Hybrid Cloud auszuschöpfen.

Kernpunkte

- Jedes Unternehmen ist ein datenbasiertes Unternehmen, und die Kosten für das Nicht-Sichern dieser Daten – sowohl logisch als auch physisch – können verheerend sein.
- On-Premise-Rechenzentren haben vielen Unternehmen bisher gute Dienste geleistet, sind aber für die Anforderungen einer Cloud-basierten Geschäftswelt im 24/7-Betrieb schlecht ausgestattet.
- Sicherheit ist für die meisten Unternehmen keine Kernkompetenz. Daher können die Herausforderungen bei der Aufrechterhaltung der physischen Sicherheit auf Unternehmensebene interne Mitarbeiter überstrapazieren und Schwachstellen öffnen.
- Interxion Cloud Connect bietet Unternehmen eine private, hochleistungsfähige und kosteneffiziente Verbindungen an den Cloud-Anbieter ihrer Wahl, einschließlich Microsoft ExpressRoute und AWS Direct Connect, und umgeht dabei das öffentliche Internet für die Cloud-Anbindung.
- Mit Cloud Connect als Teil einer Hybrid Cloud-Strategie gewinnt Ihre IT ein Höchstmaß an physischer Sicherheit, unterstützt durch integrierte Redundanz, mit der sich selbst die extremsten Situationen meistern lassen.

Einleitung: Von Grund auf sicher

Führende Unternehmensleiter wissen, welche Auswirkungen eine Datenverletzung auf ihr Geschäft haben kann. Jedes Jahr geben Unternehmen weltweit mehr als 90 Milliarden US-Dollar für Cybersicherheits-Software und -Services aus, um böswillige Angriffe wie Account-Hijacking, Phishing und Malware-Einschleusungen zu verhindern. Wenn solche Angriffe erfolgreich sind, können sie verheerende Auswirkungen auf die Geschäftstätigkeit eines Unternehmens, seine Beziehung zu Kunden und Interessengruppen sowie die Reputation des Unternehmens allgemein haben.

Da immer mehr Unternehmen Cloud-Services nutzen und ihr eigenes Rechenzentrum über das öffentliche Internet mit Cloud Gateways verbinden, werden logische Lösungen zur Sicherung der Daten vor Cyber-Bedrohungen immer dringender. Doch selbst mit den neuesten und besten logischen IT-Sicherheitsmaßnahmen sind Ihre Unternehmensdaten nur so sicher wie die physische Umgebung und die zum Schutz vor unbefugtem Zugriff eingerichteten Kontrollen. In der Tat sind physische Aktionen bei schätzungsweise fast einem Zehntel aller Datenverletzungen involviert.

Wenn es böswilligen Akteuren möglich ist, physischen Zugriff auf Cloud-Systeme zu erhalten, hilft auch die beste Cyber-Abwehr nichts mehr. Daten spielen in der Geschäftswelt eine immer wichtigere Rolle. Daher müssen Unternehmen garantieren, dass ihre Daten unter allen Umständen sicher bleiben. Dazu müssen sie eine sichere physische Umgebung für ihre Daten schaffen, die durch eine verlässliche Zugriffskontrolle unterstützt wird.

Aus diesem Grund gehen immer mehr Unternehmen dazu über, Anwendungen und Daten in Colocation-Rechenzentren zu hosten und zu speichern. Diese Colocation-Einrichtungen stellen eine günstige Alternative zum Hosting von Daten vor Ort oder in einem dedizierten Rechenzentrum dar und bieten niedrigere Kosten, höhere Zuverlässigkeit sowie lokalen Support rund um die Uhr. Mit zunehmender organisatorischer Priorität von physischer Sicherheit können Unternehmen geschäftskritische Daten und Hardware durch Colocation vor Verlust, Diebstahl oder Beschädigung schützen.

In diesem Whitepaper zeigen wir, wie Unternehmen mit Interxion Cloud Connect im Rahmen einer Hybrid-Cloud-Lösung sicheren und zuverlässigen Zugriff auf Cloud-Services erhalten können. Wir erläutern, was Cloud Connect ist, wie es funktioniert und wie es Ihrer Organisation helfen kann, ein Höchstmaß an physischer Sicherheit und Verfügbarkeit für den Betrieb Ihrer IT-Infrastruktur zu gewährleisten.

Wir zeigen auch, wie Cloud Connect die Anpassungsfähigkeit Ihres Unternehmens an abnormale oder unvorhersehbare Umstände beschleunigt, ohne dabei kritische Sicherheitsaspekte zu vernachlässigen oder zu kompromittieren.

ÜBER CLOUD CONNECT

Um die Vorteile digitaler Technologien der nächsten Generation für ihr Geschäft zu maximieren, benötigen Unternehmen die Agilität, Skalierbarkeit und Kosteneffizienz von Cloud-Services. Bei der Verwaltung komplexer IT-Stacks, die aus Legacy- und Cloud-Anwendungen oder unternehmensinterner und ausgelagerter IT bestehen können, wollen Unternehmen von einem flexiblen Angebot an Services, Bereitstellungs- und Implementierungsoptionen profitieren. Die Hybrid Cloud ist die perfekte Lösung, um diese Anforderungen zu erfüllen.

Mit dieser Chance sind jedoch Gefahren verbunden, und nichts behindert Innovation mehr als die damit einhergehende Bedrohung der Sicherheit. Im Rahmen eines hybriden Ansatzes wollen Unternehmen wissen, wie sie die öffentliche Cloud sicher nutzen können. Beim Zugriff auf Cloud-Dienste über eine öffentliche Internetverbindung gibt es jedoch erhebliche Herausforderungen: So müssen beispielsweise sensible Daten geschützt, Compliance-Anforderungen erfüllt oder die Anwendungs-Performance gewährleistet werden.

Die Gefahr von Datenverlusten ist in allen Organisationen und Branchen groß. Um das wahre Potenzial von Hybrid Cloud auf sichere Weise zu nutzen, benötigen Unternehmen ein Cloud-Service-Bereitstellungsmodell, das gewährleistet, dass der Zugriff auf geschäftskritische Daten in den richtigen Händen bleibt.

Cloud Connect ermöglicht Unternehmen einen schnellen, zuverlässigen und sicheren Cloud-Zugang. Durch die private Verbindung erhalten sie die benötigte Leistung und können das öffentliche Internet mit seinen inhärenten Sicherheits- und Leistungsdefiziten umgehen.

Was ist Cloud Connect?

Cloud Connect ist der Cloud-Zugangsservice von Interxion für die sichere, private Verbindung zu mehreren Cloud-Anbietern über eine einzige physische Verbindung in einem Carrier-neutralen Rechenzentrum.

Mit schnellen und sicheren Verbindungen zu Cloud-Anbietern Ihrer Wahl bietet Cloud Connect eine einfache, schnelle und kostengünstige Möglichkeit zur Erstellung hybrider und Multi-Cloud-IT-Umgebungen sowie zur Verlagerung geschäftskritischer Workloads und latenzsensitiver Anwendungen in die öffentliche Cloud. Dadurch können Unternehmen das öffentliche Internet mit seinen inhärenten Schwächen meiden, und sicher sein, dass ihre Daten direkt mit ihren Clouds verbunden sind.

Cloud Connect ist mit Carrier-Grade-Hardware ausgestattet, die eine Service-Level-Garantie von 99,999% bietet, in einer gesicherten Colocation-Einrichtung installiert ist und 24 Stunden am Tag an 365 Tagen im Jahr überwacht wird. Der Service ist in 13 europäischen Ländern mit Any-to-Any-Konnektivität über die lokalen Rechenzentren von Interxion verfügbar.

Warum Cloud Connect?

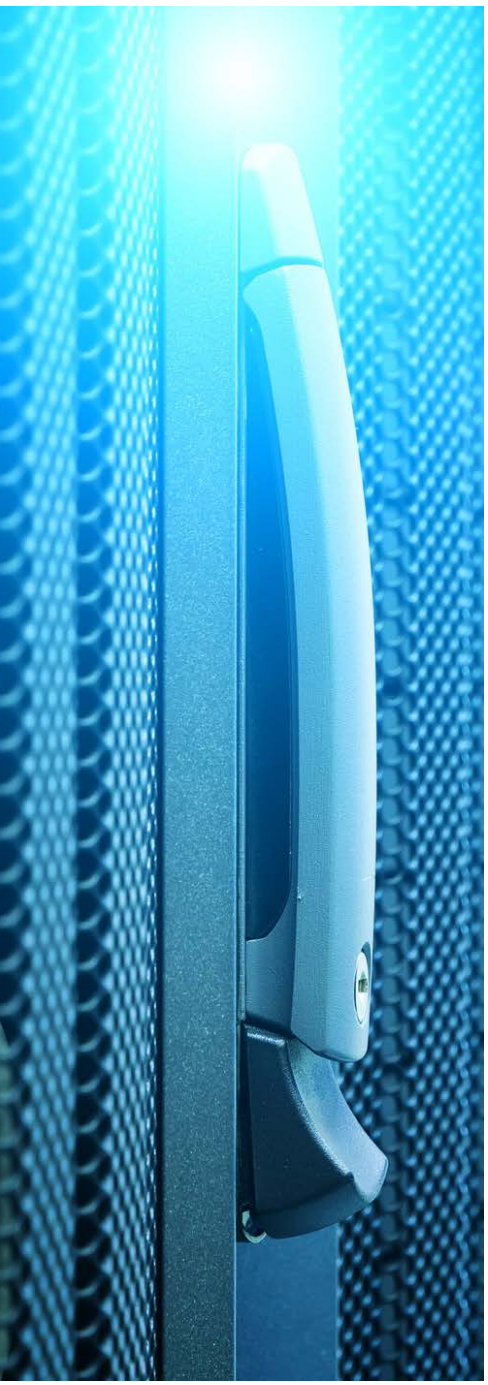
- Unterstützung mehrerer VLANs durch eine einzige physische Verbindung
- Einfache und schnelle Bestellung über unser Kundenportal
- Sichere, durch SLAs garantierte Layer 2 Connectivity
- Schnelle Bereitstellung
- Any-to-Any-Konnektivität zwischen den Interxion Niederlassungen

Cloud-Service-Anbieter

- Amazon Web Services
- City Cloud
- Google Cloud
- IBM Cloud
- Microsoft Azure
- Oracle Cloud Infrastructure

Lokale Interxion Rechenzentren

- Amsterdam
- Brüssel
- Kopenhagen
- Dublin
- Düsseldorf
- Frankfurt
- London
- Madrid
- Marseille
- Paris
- Stockholm
- Wien
- Zürich



PHYSISCHE DATENSICHERUNG

Für die meisten modernen Unternehmen sind Daten eines ihrer wertvollsten Vermögenswerte, denn durch sie unterscheiden sie sich vom Mitbewerb. Sie verkörpern auch Vertrauen – Kunden und andere Interessengruppen haben ihre Daten gegen das Versprechen weitergegeben, dass diese sicher und nur für bestimmte Zwecke verwendet werden.

Wenn Sie die physische Integrität dieser Daten und der Anwendungen, die sie ausführen, nicht garantieren können, sind diese Beziehungen gefährdet. Um dies zu verhindern, bietet Cloud Connect die höchstmögliche physische Sicherheit.

On-Premise-Rechenzentren und ihre Schwächen

Herkömmlicherweise machte es Sinn für Unternehmen, ihre Daten vor Ort zu verwalten. Dank der Nähe zum lokalen Netzwerk und internen IT-Team haben sie volle Transparenz und Kontrolle über ihre IT-Umgebung.

Physische Datenkontrolle ist aber nicht gleichbedeutend mit Sicherheit. Da die Menge und Geschwindigkeit der von Organisationen verwalteten Daten weiter wächst und immer mehr Unternehmen auf Cloud-basierte Anwendungen und Dienste zugreifen müssen, beginnt die Logik der Aufrechterhaltung eines On-Premise-Rechenzentrums zu wanken.

Abgesehen von den Leistungs- und Sicherheitsdefiziten des öffentlichen Internets ist die IT vor Ort auch hinsichtlich physischer Sicherheit anfällig. Die Server müssen rund um die Uhr gewartet und überwacht werden, der Zugang zum Serverraum bedarf strenger Autorisierung, und Zutrittslogs müssen zu Prüfzwecken aufbewahrt werden. Dies stellt eine enorme Belastung für die internen Mitarbeiter dar, die kontinuierlich und konsistent entsprechende Kontrollen durchführen müssen, und verbraucht zudem wertvolle Unternehmensressourcen.

Für die meisten Organisationen ist dies einfach nicht praktikabel. Unternehmen haben bereits genug damit zu kämpfen, den laufenden Geschäftsbetrieb aufrechtzuerhalten, und so kann die Sicherheit leicht in den Hintergrund rücken, wenn unmittelbarere Prioritäten gesetzt werden müssen.

Schaffung einer sicheren Umgebung

Cloud Connect adressiert all diese Schwachpunkte und bietet robuste physische Sicherheit und strikteste Zugriffskontrollen.

Je mehr Sicherheitsebenen ein Rechenzentrum zwischen Personen und den Datenservern bereitstellt, desto geringer ist die Wahrscheinlichkeit eines unerlaubten physischen Zugriffs. Die Rechenzentren von Interxion sind in der Regel mit fünf Sicherheitsebenen ausgestattet, sodass sie weniger anfällig für Sicherheitslücken sind. Zu diesen Ebenen gehören die Umzäunung, das Sicherheitstor und Eingangsportal, Sicherheitsschleusen am Eingang in das Rechenzentrum, Zutrittskontrollsysteme sowie sichere, verschlossene Racks. Zusätzliche Sicherheitsstufen können eingerichtet werden, z. B. abschließbare Cages oder Cold Cubes.

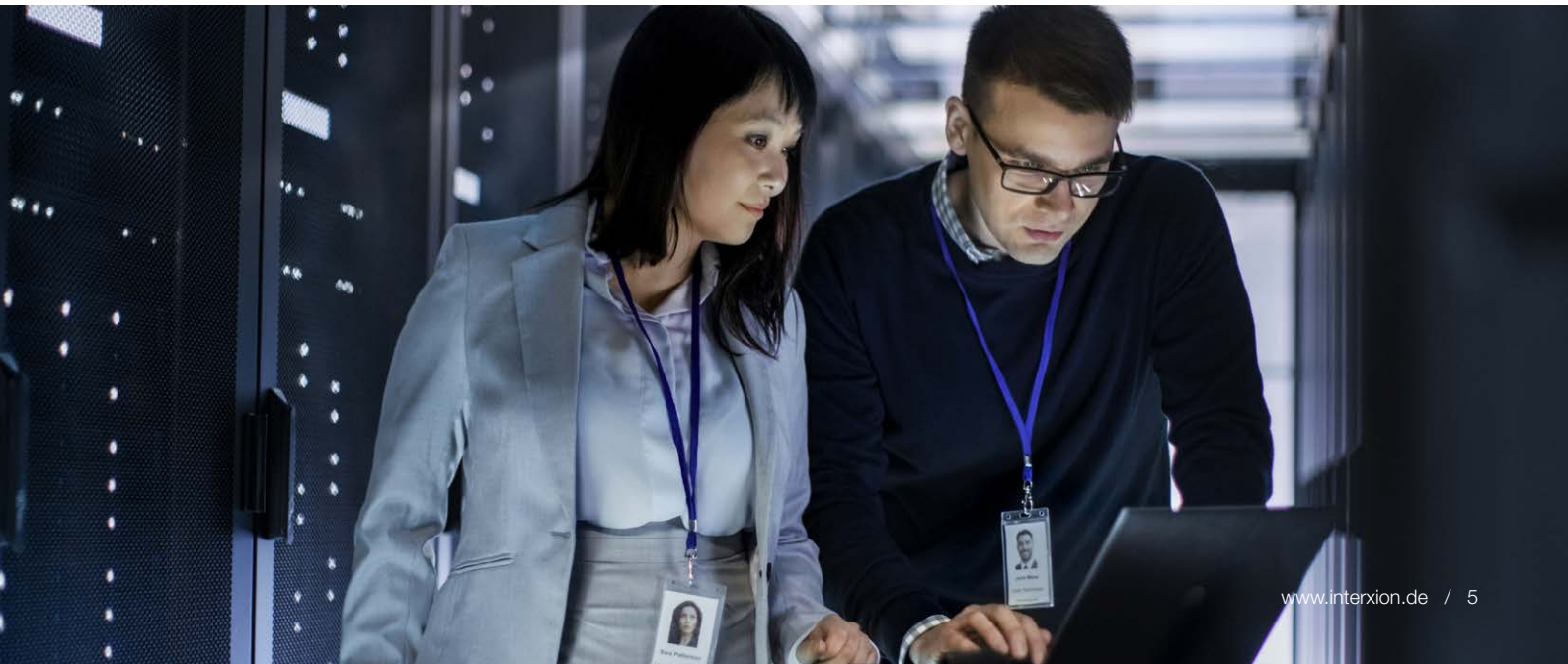
Darüber hinaus werden die Colocation-Standorte rund um die Uhr von Sicherheitsexperten bewacht. Sie kümmern sich um die Sicherheit Ihrer Hardware, sodass Sie und Ihre Mitarbeiter sich keine Sorgen machen müssen. Indem Sie die Sicherung Ihrer Daten Experten überlassen, die sich voll auf den Schutz Ihrer Server konzentrieren, können Sie Ihre Mitarbeiter entlasten und eine nachhaltigere Kostenstruktur rund um das Rechenzentrumsmanagement schaffen.

Fünfschichtiges Interxion-Sicherheitskonzept

- Geschultes Sicherheitspersonal rund um die Uhr vor Ort
- Sicherheitsumzäunung des gesamten Rechenzentrumskomplexes
- Mehrere physische Sicherheitsebenen einschließlich Proximity-Karten, biometrischen Scans, CCTV, Sicherheitsschleusen
- 24-Stunden-Zugangsüberwachung
- Informationssicherheits-Managementsystem nach ISO/IEC 27001 zertifiziert

Das physische Sicherheitskonzept mit mehreren Ebenen umfasst strenge Zugangskontrollen. Niemand kann die Interxion-Rechenzentren ohne Identitätsnachweis betreten oder verlassen, alle Besucher werden anhand von kundenspezifischen Zugangslisten überprüft und beim ersten Besuch einer Person werden biometrische Daten erfasst. Der individualisierte Zugang zu Räumen und Cages gewährleistet, dass die strikten Zugangsregeln innerhalb des gesamten Komplexes gewahrt sind. Darüber hinaus sind alle Gebäudebereiche durch CCTV und ein Alarmsystem gesichert, und ein vertragsgebundenes, lizenziertes Sicherheitsunternehmen patrouilliert das Areal sowohl innen als auch außen.

Da alle potenziellen Schwachstellen abgedeckt sind, können Sie selbst Ihre geschäftskritischsten Daten in den Rechenzentren von Interxion in der Gewissheit speichern, dass diese rund um die Uhr sicher sind.



VORBEREITUNG AUF UNERWARTETE EREIGNISSE

Es ist nicht ungewöhnlich, dass Unternehmen bei der Aufrechterhaltung ihres Rechenzentrumsbetriebs plötzlich mit unvorhergesehenen Schwierigkeiten konfrontiert werden. Dabei kann es sich um einen Stromausfall, einen unerwarteten Anstieg der Nachfrage oder den plötzlichen Ausfall einer Fachkraft handeln. Treten diese Ereignisse einzeln auf, so sind die meisten Organisationen in der Lage damit umzugehen, ohne dass die Sicherheit beeinträchtigt wird.

Handelt es sich jedoch um ein größeres Problem oder treten mehrere unerwartete Ereignisse zeitgleich ein, gestaltet sich die Neuzuordnung von Ressourcen schwieriger. In extremen Situationen, wie bei einem Notfall oder einer Naturkatastrophe, kann die physische Sicherheit des Rechenzentrumsbetriebs eines Unternehmens bedroht sein.

Die Risiken eines IT-Ausfalls

In einem solchen Fall könnte ein On-Premise-Rechenzentrum – ebenso wie die einzuhaltenden Sicherheitsprotokolle – ernsthaft gefährdet sein. Ohne Zugang zu den regulären Systemen, müssen Mitarbeiter oft gewissermaßen im Blindflug auf Ereignisse reagieren. Es kann auch gut sein, dass das an diesem Tag anwesende Personal nicht über die spezifischen Fähigkeiten verfügt, um mit dem Problem umzugehen, wodurch auf externe Unterstützung zurückgegriffen werden muss, die aber möglicherweise nicht sofort zur Verfügung steht.

Selbst im günstigsten Fall führt eine solche Situation zu längeren Ausfallzeiten, was für Mitarbeiter und Kunden gleichermaßen frustrierend ist. Schlimmstenfalls setzt sich das Unternehmen dadurch bösartigen Akteuren aus, ohne dass die normalen Abwehrmaßnahmen, die es ergriffen hat, um solche Angriffe zu verhindern, in Kraft treten.

Gut vorbereitet für alle Fälle

Cloud Connect bietet eine starke Notfallplanung und Ressourcen, die die Integrität von Geschäftsabläufen gewährleisten und es Unternehmen ermöglichen, ihr normales Tagesgeschäft ungestört weiterlaufen zu lassen.

Um eine rasche Wiederherstellung nach einem Notfall zu gewährleisten, sind die Interxion-Rechenzentren so robust und redundant wie möglich ausgelegt. Dank eingebauter Mechanismen, die selbst den schwierigsten Situationen standhalten, verfügen die Einrichtungen über eine mehr als ausreichende Redundanz, um einer „direkten Attacke“ auf die Service-Infrastruktur zu trotzen, und so kommt es in den meisten Fällen zu keinen Ausfallzeiten oder Serviceunterbrechungen. Die Anlagen verfügen über eine eigene Kühlung und redundante Stromversorgung, um einen kontinuierlichen Betrieb zu gewährleisten, und das Facility Management kann die Infrastruktur eines Kunden isolieren, wenn der Verdacht besteht, dass sie eine Bedrohung für andere darstellen.

Colocation in einem Interxion-Rechenzentrum bietet Kunden zudem Zugang zu technischem Support auf Abruf, vollständige Transparenz und Sicherheit. Dazu gehören Analyseberichte und Anrufe bei allen auftretenden Problemen, auch wenn diese den Kunden nicht direkt beeinflussen. Bei größeren Problemen wird sofort eine Notfallleitung eingerichtet, über die der Kunde alle 15 bzw. 30 Minuten Updates erhält. Die Vernetzung innerhalb einer Colocation-Umgebung hat für den Kunden darüber hinaus auch noch den Vorteil, dass er schnell Zugang zu MSPs hat, die zusätzliche Services zur Aufrechterhaltung einer sicheren IT-Umgebung bereitstellen.

FAZIT

Unternehmen brauchen Kontinuität. Die Kosten eines IT-Ausfalls sind oft unternehmensweit zu spüren. IT-Störungen, die zu Datenverlust, Diebstahl oder Downtime führen, können schwerwiegende Auswirkungen haben, von denen sich ein Unternehmen oft erst nach Wochen oder sogar Monaten erholt.

Um ihre Daten sicher und resistent gegen unerwartete Vorfälle zu machen, brauchen Unternehmen eine maßgeschneiderte Lösung. Jegliche Lücke in der Überwachung, Wartung und Wiederherstellung kann die gesamte Organisation gefährden und Personen mit böswilliger Absicht einen Angriffspunkt bieten. Es ist daher wirtschaftlich sinnvoll, die Datenverantwortung – für routinemäßige Workloads bis hin zu geschäftskritischen Anwendungen – an Experten mit dem nötigen Know-how zu übertragen, damit die Datenintegrität auch unter extremsten Bedingungen gewahrt bleibt.

Cloud Connect bietet genau das. Wenn Sie Ihre Hardware in unsere Colocation-Rechenzentren verlagern, können Sie den privaten Zugriff auf mehrere Clouds aufrechterhalten sowie die Sicherheit Ihres physischen Servers rund um die Uhr gewährleisten. Mit privaten Verbindungen zu den Cloud-Plattformen Ihrer Wahl können Sie sicherstellen, dass Ihre Daten und Anwendungen nur denjenigen zugänglich sind, die Sie ausdrücklich autorisiert haben, und Ihr Unternehmen bleibt betriebsbereit, wenn das Unerwartete eintritt.

Unabhängig von Ihrer aktuellen Cloud-Kompetenz können Sie mit Cloud Connect eine erstklassige Sicherheitsumgebung für Ihre Cloud-Dienste erstellen. Cloud Connect reduziert zudem die IT-Kosten vor Ort, begrenzt die Risiken des Cloud-Zugriffs über das öffentliche Internet und bietet Zugang zu dem erforderlichen Sicherheits-Know-how, wann immer Sie es benötigen. Mit Cloud Connect können Sie die Cloud außerdem kostengünstig und risikofrei testen. Sie sind nicht an den Service gebunden und können Setup und Kontrollen an Ihre geschäftlichen Anforderungen anpassen, sodass Sie vom ersten Tag an sicher sind.

Da Ihre IT-Umgebung geregelt ist, haben Sie interne Ressourcen frei, um sich auf das zu konzentrieren, was Ihr Unternehmen wirklich ausmacht, und die Hybrid Cloud zu Ihrem Wettbewerbsvorteil zu nutzen.

Wenn Sie mehr über Cloud Connect wissen wollen und erfahren möchten, wie Sie die Vorteile der heutigen Hybrid Cloud nutzen können, laden Sie unser Produktdatenblatt für Cloud Connect herunter oder kontaktieren Sie uns unter de.info@interxion.com für einen kostenlosen Einzel-Workshop oder individuelle Experten-Beratung.

Über Interxion

Interxion (NYSE: INXN) ist ein führender europäischer Anbieter von Cloud- und Carrier-neutralen Rechenzentrumsdienstleistungen für Colocation und betreibt insgesamt 50 Rechenzentren in 13 europäischen Städten verteilt auf 11 Länder. Interxions energieeffiziente Rechenzentren sind in einem standardisierten Design errichtet und bieten ein Höchstmaß an Sicherheit und Verfügbarkeit zum Betrieb geschäftskritischer Anwendungen. Durch den Zugang zu mehr als 700 Connectivity-Anbietern, 21 europäischen Internetaustauschknoten und den führenden Cloud- und Media-Plattformen an seinen Standorten hat Interxion Hubs für Cloud, Content, Finance und Connectivity geschaffen, welche die Etablierung von Ökosystemen für Branchen-Cluster nachhaltig fördern. Weitere Informationen über Interxion finden Sie unter **www.interxion.de**

Rechenzentrums-Dienstleistungen in Europa

www.interxion.com
customer.services@interxion.com/de

Interxion Frankfurt
Tel.: +49 69 40147 0
E-Mail: de.info@interxion.com

Interxion Düsseldorf
Tel.: +49 211 7496670-0
E-Mail: de.info@interxion.com

European Customer Service Centre (ECSC)
Tel. für Kunden aus Europa (kostenlos): + 800 00 999 222
Tel. für Kunden aus den USA (kostenlos): 185 55 999 222
E-Mail: customer.services@interxion.com