Sicher, sicherer, am sichersten

Colocation: IT im Hochsicherheitstrakt

Doris Piepenbrink

Vor allem mittelständische Unternehmen verlagern zunehmend ihre Informationstechnik (IT) in die Rechenzentren von Colocation-Anbietern. Ein wichtiger Punkt für diese Entscheidung sind die hohen Sicherheitsstandards in diesen Rechenzentren. Und manche davon sind noch ein bisschen sicherer als der Wettbewerb.

Doris Piepenbrink ist freie Journalistin in München

Die Information Services Group (ISG) stellt in ihrem im Juli 2019 veröffentlichten ISG-Report „Provider Lens – Private/Hybrid Cloud – Data Center Solutions & Services Germany 2019" eine steigende Nachfrage nach Colocation-Services fest, die weit über den Knotenpunkt Frankfurt hinaus geht. Die Nachfrage nach Flächen in Colocation-Rechenzentren zieht weiter an und hat mittlerweile alle größeren Wirtschaftsräume in Deutschland erfasst.

Während Großkonzerne zunehmend auf umfassende Cloud-Infrastrukturen setzen, verlagert demnach vor allem der Mittelstand IT-Kapazitäten in Colocation-Rechenzentren. Das betrifft oft hochspezialisierte IT- und Branchenlösungen, die sich nicht in eine Cloud verlagern lassen, sondern weiterhin auf dedizierten Servern laufen müssen. Colocation bietet die Möglichkeit, sie in eine moderne hybride Infrastruktur zu integrieren. Denn auch Anbieter von Cloud-Lösungen haben ihre Services oft auf Servern in Colocation-Rechenzentren zu laufen.

Colocation-Anbieter stellen meist vielfältige Anbindungsmöglichkeiten und umfangreiche Schutzmaßnahmen zur Verfügung, was mit eigenen Rechenzentren zu vertretbaren Kosten kaum realisierbar ist. Hauptauswahlkriterien für IT-Abteilungen sind somit neben den Kosten vielfältige und schnelle Anbindungsmöglichkeiten für kurze Antwortzeiten und hohe Redundanz sowie möglichst umfangreiche Sicherheitsvorkehrungen. Dabei steigen mit zunehmender Ausfallsicherheit natürlich die Kosten.

Nicht nur Hacker, Trojaner und Computerviren, sondern auch unerlaubter physischer Zugriff auf Datenträger stellen eine Gefahr dar. Für Torben Belz, Geschäftsführer des Bremer Colocation-Anbieters Plutex, beginnt die Datensicherheit bereits bei physischen Kontrollen. Dazu nutzen Rechenzentren u.a. Zufahrtskontrollen zum Gelände sowie Mehrfachauthentifizierungssysteme für die Eingangstür. Er erklärt: „Bei uns können lediglich Server-Eigentümer sowie autorisierte Mitarbeiter die Server-Räume betreten. Jeder muss seinen Besuch zuvor anmelden und sich über einen persönlichen Chip und eine individuelle PIN-Nummer authentifizieren. Dadurch erfolgt auch eine automatische Dokumentation dessen, wer sich wann und wie lange im Gebäude befand. Videoaufzeichnungen und Gesichtsabgleich dokumentieren darüber hinaus alle Zutritte, so dass sich Auffälligkeiten auch im Nachgang über das Archiv nachvollziehen lassen." Als letzter Schritt versperren Sicherheitsschlösser die Serverschränke, so dass der Zugriff nur für Eigentümer möglich ist. Auch bei der Entwicklung und Installation der einzelnen Komponenten für das Zutrittsmanagement setzt das Unternehmen auf eigene Mitarbeiter, damit keine Unbefugten an digitale oder physische Zutrittsdaten und -komponenten gelangen können. Bei den biometrischen Verfahren sind neben Gesichtserkennung oft auch Handvenenscanner im Einsatz wie z.B. bei Telehouse KDDI, Equinix oder Fujitsu.

Die 3U-Rechenzentren in Berlin und Hannover sind ebenfalls umfangreich mit Zutrittskontrollsystemen, Alarmanlage und Videoüberwachung ausgestattet, aber generell unbemannt. Bei ungewöhnlichen Vorkommnissen steht ein externer Wachschutz zur Verfügung, der mit einer kurzen Reaktionszeit vor Ort ist. Kunden können abgeschlossene Racks, eigene Gitterkäfige oder abgetrennte Bereiche mieten. Der Zugang zu diesen Einheiten wird individuell gestaltet. Dies fängt bei der Wandbauweise an und hört mit der Installation von kundeneigenen Sicherheitssystemen in diesen abgetrennten Bereichen auf. Grundsätzlich sind es sehr kundenindividuelle Lösungen. Dabei ist es möglich, in-

nerhalb der Käfige 3U-Sensoren zu installieren, die der Anbieter überwacht, oder eigene Überwachungssysteme einzubauen.
Britisch Telecom (BT) hat für sein Datacenter in Frankfurt-Sossenheim z.B. einen physischen Anfahrtschutz errichtet, der durch Gräben und Zäune den Rechenzentrumsperimeter zusätzlich schützt. Außerdem verwendet der Betreiber Wärmebildkameras im Außenbereich.
Auch QSC schützt seine Rechenzentren und zugehörige Gelände mit Zäunen sowie zusätzlichen Steingabionen und überwacht das Ganze mit Nachsichtkameras. Am Standort München wird sogar das gesamte Industriegelände um das Rechenzentrum videoüberwacht, und das Gebäude ist mit einem „Anfahrtschutz" ausgestattet. Der Kunde kommt bei diesem Anbieter über mindestens vier Türschließsysteme zu seiner IT. Die Cages sind mit Blick-, Übersteig- und Unterkriechschutz sowie einer Einbruchmeldeanlage (Bewegungsmelder, Tür- und Schließkontakte, Pinpad) und Zutrittskontrollanlage (Zweifaktorauthentifizierung) ausgestattet. Am Rack befindet sich eine Videoüberwachung.
Interxion hat ein fünfstufiges Sicherheitskonzept und ständig Sicherheitspersonal vor Ort. Dieser Anbieter realisiert vom verschließbaren Cage über abgetrennte Gänge (Cubes) bis hin zum „Rechenzentrum im Rechenzentrum" jede Variante des Housings.
Fujitsu betreibt einige hochsichere Rechenzentren in Deutschland, etwa in Neckarsulm und Neuenstadt am Kocher, mit einem durchgehend vor Ort befindlichen Wachdienst. Als Zutrittskontrolle für das Personal ist eine Mehrfaktorenauthentifizierung installiert. Alle weiteren Schutzmaßnahmen werden bei Fujitsu individuell für jeden Kunden entsprechend des vereinbarten Outsourcing-Konzeptes realisiert. Dabei unterscheiden sich die systemspezifischen Sicherheitsvorkehrungen etwa für den Zugriff und den Datenaustausch teilweise stark voneinander.
Auch bei Equinix können die physischen Sicherheitsvorkehrungen inkl. Cage-Überwachung entsprechend den jeweiligen Bedürfnissen ausgebaut werden. Und Mpex Berlin-NET (E-Shelter und Centurylink) setzt z.B. speziell für E-Shelter zusätzlich auf einen 24/7-Wachdienst mit ständig besetzter Rezeption. Mitarbeiter wie Besucher müssen sich mit einem amtlichen Lichtbildausweis ausweisen und diesen als Pfand hinterlegen. Gäste erhalten eine sichtbar zu tragende Besucherkarte. Beim Nürnberger Anbieter Contabo dürfen sich Kunden und Besucher nur zusammen mit dem RZ-Personal auf dem Gelände bewegen. Das Rechenzentrum ist rund um die Uhr mit technischem Personal besetzt.
Viele Anbieter integrieren bei Bedarf auch eine fernbedienbare Schranküberwachung, über die der Kunde den Zustand seiner IT selbst kontrollieren kann. Das gilt z.B. für BT, QSC, Equinix, Interxion, Mpex in Berlin oder Contabo. Telehouse KDDI hat bei seinen neueren Rechenzentren für die Gebäudeautomation und die Überwachungsdienste ein IP-Bussystem integriert, das nach eigenen Angaben „eine höchstmögliche Verfügbarkeit realisieren" soll.

Bei Equinix wie bei anderen Anbietern erstrecken sich die Sicherheitsmaßnahmen bis zum Kundenbereich. Neben Zutrittskontrollen per Kartenleser ist auch die Überwachung von Cages möglich (Foto: Equinix)

Schutz vor Hitze und Feuer

Nicht nur der bewusste Angriff auf gespeicherte Daten stellt eine Gefahr dar, sondern auch Umwelteinflüsse wie Hitze oder Feuer. Im Rechenzentrum erfolgt daher eine Kühlung der einzelnen Server rund um die Uhr. „Sollte dennoch einmal ein Feuer entstehen, gibt es einen konkreten Ablauf: Da Wasser oder Löschschaum die Server schädigen würde, verdrängt ein speziell für Rechenzentren entwickeltes Löschsystem den Sauerstoff aus dem Serverraum, so dass das Feuer erstickt wird", erklärt Torben Belz. Auch das machen mehrere Anbieter in ähnlicher Weise. So arbeitet Interxion mit Brandfrüherkennung und partiell agierenden Löschsystemen, die das IT-Equipment der Kunden nicht beschädigen.

Zertifizierungen

Die meisten Colocation-Rechenzentren erreichen in Deutschland heute nach eigenen Angaben eine Verfügbarkeitsklasse von Tier 3 oder darüber. Bei Zertifizierungen sind für Rechenzentren vor allem die TÜV-Zertifizierungen nach ISO 9001 und ISO 27001 für die Überprüfung von Qualitätsmanagement und Informationssicherheit relevant. Die meisten Colocation-Anbieter verfügen über diese Zertifizierungen, da viele Kunden diese voraussetzen.
Interxion hat darüber hinaus eine PCI-DSS-Zertifizierung für die Abwicklung von Kreditkartentransaktionen, zudem sind die Rechenzentren konform mit dem SOC-2-Selbstaudit. Bei BT sind alle europäischen Datacenter nach ISO 27001 zertifiziert. Auch sind kundenspezifische Zertifizierungen wie ISAE 3402 oder PCI-DSS möglich.
Alternativ sind Rechenzentren auch nach dem Trusted-Site-Infrastructure-Programm (TSI) des TÜViT zertifiziert. Die Rechenzentren von Equinix erreichen hier z.B. Level 3. Diese Zertifizierung deckt auch die Anforderung der EN 50600 ab und umfasst einen umfangreichen Kriterienkatalog, der Aspekte wie Umwelt, Konstruktion, Brandschutz, Sicherheit oder Verkabelung mit einschließt. Alle zukünftigen Equinix-Neubauten in Deutschland

Das Security Center von Interxion in Düsseldorf zur Überwachung von Türen, Schleusen und Gängen (Foto: Interxion)

sollen nach diesem Verfügbarkeitsstandard zertifiziert werden. Zusätzlich sind die Rechenzentren dieses Anbieters nach PCI-DSS sowie ISAE 3402 (SOC 1 und SOC 2) zertifiziert.
Die QSC-Rechenzentren in München und Nürnberg sind vom TÜV Süd für die Hochverfügbarkeitsstufe 3 zertifiziert, das Rechenzentrum in Hamburg erhielt vom TÜViT sogar eine TSI-3.2-Zertifizierung (erweitertes Level 3). Auch bei QSC haben die Rechenzentren ein ISAE-3402-Zertifikat für rechnungslegungsrelevante Prozesse. Ähnliches gilt für die Rechenzentren von Telehouse KDDI. Diese bieten zudem eine B3S-Zertifizierung für kritische Infrastrukturen an.

Verteilte und gespiegelte Rechenzentren

Vor allem die großen Anbieter wie BT, Equinix, Fujitsu oder QSC ermöglichen ihren Kunden den Einsatz gespiegelter Rechenzentren und verteilter Infrastrukturen und gewährleisten so eine ständige Hochverfügbarkeit und Zugriffssicherheit für kritische Unternehmensdaten. Bei Equinix stehen dafür sogar mehr als 200 global verteilte Rechenzentren zur Verfügung, bei Fujitsu über 150, bei BT 40. Hier bringen die gespiegelten Rechenzentren nicht nur Redundanz, sondern minimieren zudem die Latenzzeiten beim weltweiten Zugriff auf Unternehmensdaten. Bei BT werden deshalb immer wieder verteilte Hubs in Europa, Asien und in den USA für eine weltweite Serviceabdeckung nachgefragt.
3U bietet mit den Standorten Berlin und Hannover ebenfalls verteilte Rechenzentren an, wobei diese mit einer direkten redundanten Faserverbindung miteinander verbunden sind. Da diese mehr als 200 km voneinander entfernt seien, würde das laut Björn Friedrichsen, Leiter Produktmanagement & Strategie bei 3U Telecom in Hannover, auch der neuen BSI-Empfehlung entsprechen. Interxion bietet das z.B. für seine Rechenzentren in Frankfurt und Düsseldorf an. Bei BT ist es am Standort Frankfurt-Bonames möglich, IT-Lösungen redundant in zwei unterschiedlichen Brandschutzabschnitten aufzubauen. Genügt dies nicht, kann eine Georedundanz zwischen den Standorten Frankfurt-Sossenheim und Frankfurt-Bonames hergestellt werden. Ist eine größere Distanz zwischen den Standorten nötig, ist auch eine Redundanz zwischen Frankfurt und Amsterdam oder anderen BT-Standorten möglich.

Stromversorgung

Fast jedes Colocation-Rechenzentrum kann bei einem totalen Stromausfall auf dieselbetriebene Notstromaggregate zurückgreifen, die ebenfalls redundant ausgelegt sind. Bei der Auswahl des Anbieters sollte man darauf achten, dass das Rechenzentrum redundante Stromzuführungen hat, bei denen die beiden Versorgungspfade komplett voneinander getrennt geführt und jeweils mit eigener USV und Notstromaggregat ausgestattet sind. QSC hat bei seinen Rechenzentren sogar für jedes Gebäude mehrere Strompfade installiert, damit selbst innerhalb eines Rechenzentrums Server in Raum A einen vollständig anderen Versorgungspfad als die Server in Raum B erhalten.

Datennetz

Grundsätzlich sind die integrierten Datennetze in Colocation-Rechenzentren immer redundant ausgelegt. Mpex Berlin beispielsweise betreibt ein eigenes, voll redundantes Routing-Setup mit einem autonomen System auf BGP4-Basis. Zudem sind mehrere Upstream-Tier-1-Provider über jeweils getrennte Leitungswege mit Gigabit- und 10-Gigabit-Verbindungen an das Rechenzentrum angeschlossen. Ähnlich macht das auch Contabo in seinen Rechenzentren. Neben den redundanten Hauseinführungen sind auch das Core-Routing und Switching redundant (2N) ausgelegt.
Bei 3U ist das IP-Netz als Ring ausgeführt mit mehreren IP-Upstream-Partnern. Beim Ausfall eines Ringsegmentes oder eines IP-Partners gibt es keine Einschränkung für die Kunden. Lediglich die Verfügbarkeit ist für den Zeitraum der Störung geringer.
Große Colocation-Anbieter im Frankfurter Raum bieten hier oft noch mehr Auswahl. Bei Interxion sind es über 200, bei Equinix sollen es sogar über 500 Carrier sein, die jeweils redundant angebunden sind. Darüber hinaus sollten die Rechenzentren Direktverbindungen zu einem oder mehreren deutschen Internetknoten haben, um ihren Kunden eine schnelle Anbindung gewährleisten zu können.
Der sichere Datenzugriff wird i.d.R. per VPN (Virtual Private Network) realisiert. Bei 3U beispielsweise kann IPsec VPN über einen Managed-Firewall-Dienst hinzugebucht werden. Dieser Anbieter hat darüber hinaus für mobile Mitarbeiter und Home-Office-Arbeitsplätze spezielle VPN-Zugänge mit Zweifaktorauthentifizierung im Programm. Das können Zugänge zu einer Private Cloud oder in ein privates Netz im Colocation-Rack sein. 3U überwacht und betreut diesen Dienst.
Mpex Berlin bietet einen SSH-Fernzugriff auf Linux-Systeme an mit Public/Private-Key-Authentifizierung und eingeschränktem IP-Adressraum. Bei diesem Anbieter kann der Kunde auch eine Datenhaltung auf vollverschlüsselten Datenträgereinheiten beauftragen. Da QSC auch Carrier ist, kann dieser Colocation-Anbieter dedizierte MPLS-Leitungen zwischen Colocation-Rechenzentrum und Unternehmensstandorten anbieten. Ansonsten

läuft die Kommunikation über VPN-Verbindungen.
Auch die BT-Rechenzentren sind über das eigene Glasfasernetz verbunden. Der Kunde erhält eine redundante Anbindung an zwei MPLS-PoPs (Points of Presence) und zwei Internet-PoPs in Frankfurt. BT bietet verschlüsselten Zugriff per MPLS, Ethernet-WAN sowie Internet. Standard ist IPsec, aber auch alle anderen marktbedeutenden Verschlüsselungslösungen werden kundenspezifisch unterstützt. In Großstädten wie Frankfurt betreibt BT sogar eigene Glasfasernetze, so dass die beiden BT-Rechenzentren in Frankfurt wegeredundant über zwei unterschiedliche Glasfaserringe verbunden sind, die nahezu beliebige Bandbreiten erlauben. Durch die geringe Latenz ist hier auch ein Betrieb von Active-Active-Konfigurationen möglich, bei denen die Kundenapplikationen gleichzeitig in beide Rechenzentren Daten schreiben und bei Ausfall eines Systems ohne Downtime oder Datenverlust weiter arbeiten können. Größere Distanzen zwischen Städten, Ländern und Erdteilen überbrückt BT über das eigene weltweite MPLS-Netz.

Cloud-Anbindung

Um gehostete Cloud-Lösungen sowie Verbindungen zu diesen Lösungen zu schützen, nutzen einige Anbieter wie BT, QSC oder Equinix Anti-DDoS-Lösungen. Bei Contabo ist der DDoS-Schutz ohne Zusatzkosten im Servicevertrag enthalten. Auch bei Telehouse KDDI sind sämtliche Verbindungen ins Internet per DDoS-Lösung und Firewall geschützt. Nach eigenen Angaben verfügt Equinix zudem über eine eigene Schaltstelle mit dem Produkt „Equinix Cloud Exchange". Kunden sollen darüber „mit verschiedenen Schutzoptionen" auf die Dienste der angebundenen Cloud-Anbieter zugreifen können. Interxion bietet spezielle Sicherheitsmechanismen in agilen Cloud-Umgebungen über die Verschlüsselungslösung „Key Guardian".
QSC und BT bieten MPLS-Verbindungen zu Cloud-Anbietern an. BT nennt die Verbindungen „BT Cloud Connect", sie sind für alle gängigen Anbieter wie AWS, Google Cloud, MS Azure, Salesforce oder Oracle buchbar. Hinzu kommen Security Services wie Firewall und Intrusion-Detection-Systeme bis hin zu gemanagten SIEM-Services (Security Incident & Event Management), bei denen die Kundenumgebung rund um die Uhr überwacht und bei Cyberattacken mit dem Kunden abgesprochene Gegenmaßnahmen eingeleitet werden. Speziell für seine deutschen Kunden betreibt BT dazu ein Security Operations Center in Eschborn. Bei BT sind beispielsweise auch Schwachstellenanalysen für Kundenplattformen per Ethical Hacking (Penetration Testing) möglich.
3U greift bei dieser Thematik und anderen spezifischen Schutzsystemen auf Partner zurück, um eine passende Lösung für den Kunden bereitstellen zu können. Ähnliches gilt für den Berliner Anbieter Mpex.

Die Internetserver von Contabo im Nürnberger Rechenzentrum. Als Hoster bietet dieser Provider auch Rechenkapazitäten auf eigenen Servern an. Dieses RZ ist derzeit mit knapp 20 x 10 Gbit/s mehrfach redundant an das Internet angeschlossen: über zwei unterschiedliche Hauseinführungen an mehrere Provider wie Centurylink, Telia oder Versatel (Foto: Contabo)

Zusätzliche IT-Dienste

Telehouse KDDI bietet nicht nur Housing-Services an, sondern auch erweiterte IT-Dienste inklusive Services für Cloud-Lösungen. Das Service-Team dieses Anbieters ist rund um die Uhr vor Ort und übernimmt auch „Remote Hands Services", agiert also als verlängerter Arm für die IT-Abteilung des Kunden. Einen ähnlichen Dienst bietet auch 3U unter dem Namen „Managed Colocation" an.
Contabo betreibt in seinen Rechenzentren in Nürnberg und München für das Outsourcing von Kunden-IT nach eigenen Angaben „nahezu 100.000 dedizierte oder virtuelle" eigene Serversysteme. Auch reine Colocation-Kunden profitieren da vom Know-how und Verständnis für spezielle IT-Bedürfnisse sowie von günstigen Preisen bei der Internetanbindung.

Sicherheitskonzept

Führende Colocation-Provider halten ein umfangreiches Sicherheits- und Business-Continuity-Konzept vor, um auf alle Eventualitäten geeignet reagieren zu können. Dazu zählt z.B. Interxion. Dieser Anbieter hat hier aus Sicherheitsgründen auch so gut wie keine Angaben zur Ausführung und Absicherung der Anbindung seiner Rechenzentren gemacht. Und Equinix prüft das eigene Security-Konzept mindestens einmal im Jahr, gleicht es mit den neuesten Techniken und Anforderungen ab und passt das Security-Konzept entsprechend an. Das physische und logische Sicherheitsmanagement der BT-Rechenzentren wird ebenfalls kontinuierlich verbessert und regelmäßigen internen und externen Audits unterzogen.

Fazit

Colocation umfasst nur die Vermietung von abgesicherten Rechnerräumen. Und schon da kann der Serviceumfang sehr ausgefeilt und individuell sein. Eine durchgängig redundant ausgelegte Anbindung mit umfassend überwachten Räumlichkeiten hat natürlich ihren Preis. Das mag für einige geschäftskritische Anwendungen sinnvoll sein, aber wohl nicht für alle Server. Wer sich für einen Anbieter entscheidet, der ein eigenes Glasfasernetz und/oder Cloud-Plattformen betreibt, kann den Serviceumfang über das Housing hinaus noch deutlich ausbauen. *(bk)*