Eine Sorge weniger!

Als das Bremer Entsorgungsunternehmen Nehlsen AG im vergangenen Herbst seinen Standort innerhalb der Hansestadt wechselte, war eines klar: Auch die IT-Strukturen mussten den alten Standort in der Furtstraße verlassen. Zur Wahl stand der Bau eines eigenen Rechenzentrums oder die Suche nach einem Colocation-Partner. Das Rennen machte die ColocationIX GmbH mit ihrem Hochsicherheits-Datacenter im umgebauten Atomschutzbunker. Nach einem Jahr neue Datenheimat zieht Nehlsen Bilanz.

Ein Unternehmen und seine IT-Strukturen

Die Nehlsen AG ist die Konzernholding des mittelständisch geprägten Nehlsen-Konzerns, der mit seinen 2.500 Mitarbeitern in den Bereichen Entsorgung, Logistik und Sicherheitsdienstleistungen national sowie international tätig ist. Innerhalb der Nehlsen AG agiert die IT-Abteilung vom Bremer Standort aus als zentraler IT-Dienstleister für alle Tochterunternehmen im Konzern. Zu den Leistungen gehören ein zentral aufgestellter Rechenzentrumsbetrieb, das Management aller Systeme und Firmennetze, die zentrale Bereitstellung der Softwareanwendungen sowie die Betreuung der circa eintausend Anwender innerhalb Deutschlands. Diese erfahren zu allen Softwareprodukten, die Nehlsen nutzt, Unterstützung über einen zentralen Helpdesk. Zudem hosten die IT-Mitarbeiter das ERP-System, alle Office- und Kommunikationstools, Dokumentenmanagement-Systeme, BMI-Tools, die HR- und Finance-Software sowie Branchenlösungen für den Bereich Entsorgung. Darüber hinaus entwickelt und programmiert das Team eigene firmenspezifische Softwareanwendungen. Nehlsens firmeninternes IT-Team umfasst rund dreißig Mitarbeiter inklusive Auszubildender. Innerhalb der Strukturen bildet der Rechenzentrumsbetrieb einen eigenen Bereich ab – ihn verantwortet Florian Moje. Der ausgebildete IT-Systemelektroniker und Bachelor in „Wirtschaft und Management" arbeitet bereits seit 2002 im Unternehmen und bekleidet seit 2010 die Position Teamleiter im Rechenzentrum.

Vorher: Das eigene Rechenzentrum stößt an seine Grenzen

Die IT-Abteilung der Nehlsen AG betrieb bis Mitte 2017 zwei redundante Rechenzentren am Standort Bremen-Grohn in Eigenregie, an deren Servern alle circa 50 bis 60 Nehlsen-Standorte in Deutschland via Multiprotocol-Label-Switching(MPLS)-Übertragung sowie Internet angebunden waren. Fünfzig Außenstellen mit eintausend Anwendern, die darauf angewiesen waren und sind, dass die Serverstrukturen zuverlässig performen. Um dies zu gewährleisten, kümmerten sich die IT-Mitarbeiter eigenhändig um

die Wartung der Infrastrukturkomponenten wie zum Beispiel die unterbrechungsfreie Stromversorgung (USV), Klimaanlagen und um die Sauerstoffreduktionsanlagen für die Serverräume. Insbesondere Letztere zeigte sich wartungs- und kostenintensiv. Die nicht mehr zeitgemäße Anlage erforderte es, dass sich fünf IT-Mitarbeiter circa zwanzig Stunden pro Monat darum kümmerten, das System am Leben zu halten. Alles lief auf eine zeitnahe Komplett-Modernisierung hinaus – verbunden mit hohen Investitionskosten.

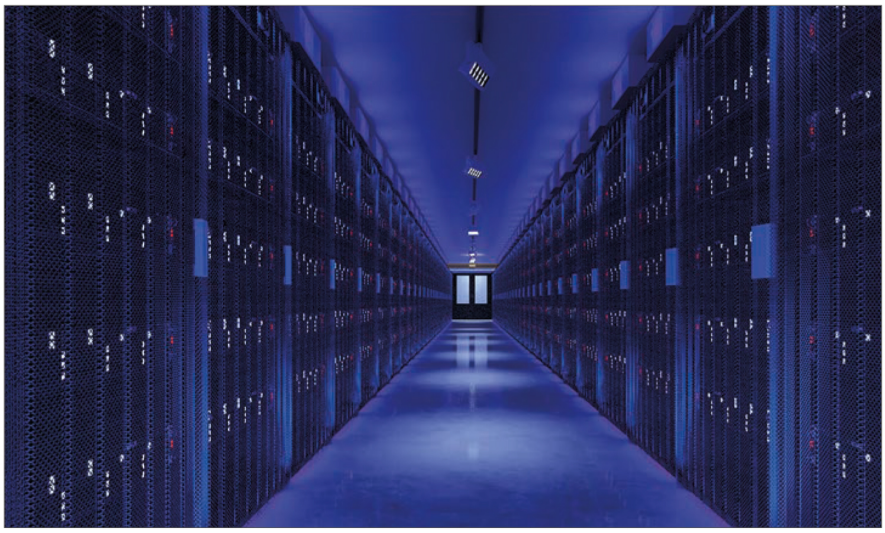
Die Entscheidung

Aufgrund einer Verlegung des Firmensitzes innerhalb Bremens musste die IT-Abteilung 2017 auch Räumlichkeiten für ein neues Rechenzentrum finden. Die Geschäftsführung und die IT-Leitung standen vor der Entscheidung, erneut ein eigenes redundantes Rechenzentrum am neuen Standort zu bauen oder die Aufgabe an einen Colocation-Anbieter abzugeben. Dabei bezeichnet der Fachbegriff Colocation die Unterbringung und Anbindung eigener Server in einem externen Rechenzentrum. Unter Abwägung von Zeit und Effizienz entschied sich die Nehlsen AG für den externen Partner. Florian Moje legte bei der Suche nach einem neuen Zuhause für die Server Wert auf Ausfallsicherheit und eine gute Netzanbindung an große lokale sowie internationale Provider, deren Peerings für genügend Bandbreite, eine geringe Latenz sowie einen reibungslosen Datenaustausch sorgen. Auch die Einbruchsicherheit spielte eine große Rolle. Da der Konzern mit seinen Dienstleistungen auch an öffentlichen Ausschreibungen teilnimmt und hierfür jeweilige Zertifizierungen von Vorteil sind, galt es bei der Wahl entsprechende Normen und Standards nach ISO 27001 einzuhalten. Für Nehlsen kam ausschließlich ein IT-Dienstleister infrage, der durchgängig ISO 27001 zertifiziert ist und damit die Qualitäts- und Prüfkette stringent fortsetzt.

Neue Serverheimat ColocationIX

Zeitgleich zur Verlegung des Nehlsen-Firmensitzes entstand im Bremer Westend mit ColocationIX ein neues Hochsicherheits-Rechenzentrum der Kategorie „Mittleres Rechenzentrum". Das Datacenter ist in einem umgebauten Atomschutzbunker untergebracht und bietet auf 2.500 Quadratmetern Raum für bis zu 50.000 Server. Seine Planung erfolgte auf Basis der US-Rechenzentrumsnorm TIA942 Tier4, der neuen Europäischen Rechenzentrumsnorm EN50600 Klasse 4 sowie der Norm ISO 27001 für Informationssicherheit. Damit entspricht die Sicherheits-Architektur des Datacenters den Anforderungen Kritischer Infrastrukturen (KRITIS).

Zwischen Uwe Jambroszyk, dem Sales Director der ColocationIX GmbH, und der IT-Leitung der Nehlsen AG bestand zu diesem Zeitpunkt bereits regelmäßiger Kontakt und nach einigen Meetings stand fest, dass die Nehlsen AG in das Rechenzentrum der ColocationIX einziehen wird. Der Umzug fand im September 2017 statt. Ihm ging eine zwei- bis dreimonatige Planungsphase sowie eine vierwöchige konkrete Vorbereitungsphase voran. Den Umzug selbst setzte das Team von Florian Moje mit Unterstützung der ColocationIX-Mitarbeiter entspannt innerhalb eines Wochenendes um.



c.l.n.r.: Gabriel Kyle, Uwe Jambroszyk, Florian Moje, Andres Dickehut, Axel Plaßmeier

Alle Bilder: ColocationIX

Der Bau eines eigenen neuen Rechenzentrums hätte Investitionskosten von circa 200.000 € erzeugt und viele personelle Ressourcen des IT-Teams gefordert. Marktrecherchen, Beauftragung und Überwachung von Dienstleistern und der Bau selbst hätten die Inbetriebnahme zudem um mindestens drei Monate nach hinten verlagert. „Einen vergleichbaren Standard zu dem, was uns heute ColocationIX bietet, hätten wir mit einer eigenen Lösung zudem niemals erreicht", weiß Florian Moje.

Aufgeteilt in zwei separate Brandabschnitte leisten rund dreißig physikalische und dreihundert virtuelle Server ihren Dienst, während sie über redundante Glasfaser an das Nehlsen-MPLS-Netz angebunden sind. Den neuen, zehn Kilometer entfernten Firmensitz in der Wilhelm-Karmann-Straße band das Team von ColocationIX mithilfe einer sogenannten Dark-Fiber-Leitung inklusive eines modernen passiven DWDM-Multiplexverfahrens breitbandig mit maximal 44x 10GbE an das Rechenzentrum von ColocationIX an.

Gute Gründe

In der hohen physikalischen Sicherheit und der damit verbundenen Ausfallsicherheit, die das Rechenzentrum im ehemaligen Atomschutzbunker bietet, sieht Florian Moje den Hauptgrund für den Wechsel zu ColocationIX. „Das Konzept der Sauerstoffreduktion zur Brandvermeidung sowie die unterbrechungsfreie Stromversorgung und zusätzliche Notstromgeneratoren haben uns überzeugt", berichtet der Rechenzentrumsleiter. „Unsere Anwender greifen remote auf die zentral im Rechenzentrum gelagerten Daten zu und haben meist kaum oder im Idealfall gar keine lokale Software mehr auf den Arbeitsrechnern und Notebooks installiert. Daher muss das Datacenter umso mehr eine sehr hohe Verfügbarkeit sowie Performance bieten. Hierfür muss sowohl die gesamte, zentralisierte Server-Infrastruktur im Nehlsen-Rechenzentrum als auch die WAN-Anbindung an die Außenstellen redundant ausgelegt sein."

Als weiterer Entscheidungspunkt kommt das umweltfreundliche Energie-Konzept der Anlage ins

Spiel, denn Umweltschutz und ökologische Nachhaltigkeit sind auch der Geschäftsführung und dem Vorstand der Nehlsen AG sehr wichtig. So laufen sowohl deren Entsorgungsfahrzeuge als auch die Pkw-Flotte teilweise bereits mit neuen Hybrid- sowie Elektro-Antrieben.
Das hohe digitale und physische Sicherheitskonzept kombiniert mit dem innovativen Brandschutzsystem und der geothermalen Kühlung von ColocationIX passt exakt zur Unternehmensphilosophie von Nehlsen.
Das Rechenzentrum im Bremer Hochbunker bietet höchste Energieeffizienz und wurde im Jahr 2014 mit dem Deutschen Rechenzentrumspreis für Energieeffizienz und im vorigen Jahr mit dem eco://award 2018 in der Kategorie Datacenter Infrastructure ausgezeichnet. Dank den externen und internen Kühl-Systemkomponenten schaffen mehrere voneinander unabhängige Kreisläufe die gewünschte Redundanz. Insbesondere die Kombination überirdischer Systeme mit unterirdischen Geothermie-Systemen macht ColocationIX dabei noch sicherer.

Effizient trotz permanenter Sauerstoffreduktion und großzügig dimensionierter USVs

Bei durchschnittlichen Rechenzentren liegt der Power-Usage-Effectiveness(PUE)-Wert – er gibt das Verhältnis aus Gesamtenergieverbrauch und Energieverbrauch der IT betrachtet über ein Jahr an – bei circa zwei. Bei einem Verfügbarkeitsanspruch beruhend auf der europäischen Rechenzentrums-Norm EN 50600 Klasse 4 setzt ColocationIX auf einen PUE-Wert von 1,05, basierend auf der Leistung von einem Megawatt.
Dazu gehören die permanente Sauerstoffreduktion sowie eine lange Batterielaufzeit der USV-Anlagen. Beides führt zu einem erhöhten Energiebedarf, der allerdings durch das innovative Kühlsystem stark relativiert wird. Bei einer Größenordnung von einem Megawatt spart ColocationIX damit rund 95 Prozent der Energie für den Anteil der Kühlung. Somit erreicht das neue Bremer Rechenzentrum einen absoluten Spitzenwert und zeigt, dass Grün spart, ohne bei der Leistungsfähigkeit Einschränkungen hinnehmen zu müssen.

In den Tiefen der Erde

Darüber hinaus lässt sich durch die Nutzung von Grundwasserzirkulation die Abwärme effizient kühlen, denn die Verfügbarkeit der „Erdkälte" ist jederzeit zu 100 Prozent gegeben – unabhängig von Wind und Wetter.
Selbst länger anhaltende Hitzeperioden verändern die Temperaturen in 100 bis 200 Meter Tiefe nicht. Um das Prinzip dieser Grundwasserzirkulation zu nutzen, hat man im Bremer Hochbunker spezielle Sonden 100 und 200 Meter tief in die Erde gebohrt. In der Hitzeperiode, in der Kältemaschinen ihren höchsten Stromverbrauch hätten, liefern die Sonden kostengünstige Kühlung. Diese Kühlung erfolgt unter minimalem Stromverbrauch, ganz ohne Kältemaschine.

Außerhalb der Hitzeperiode wird die Umgebungsluft als Kältequelle eingesetzt. Mehrere Rückkühler auf dem Dach führen dabei die Kälte in den Erdboden zurück, um die Geothermie zu regenerieren. So wird der Untergrund als Kältespeicher über die Sonden immer wieder mit Kälte aufgeladen und kann damit in der Kühlphase maximal ausgeschöpft werden.

In den Übergangszeiten werden die Rückkühler adiabatisch, also mit Wasserbenebelung, betrieben. So liefern Sie Temperaturen unterhalb der Umgebungstemperatur. Steigen die Außentemperaturen auf über 20 Grad Celsius, so werden die Rückkühler mit Wasser benebelt. Sie kühlen dadurch um mehrere Grad ab, sodass das Kühlwasser auf unter 20 Grad gekühlt wird.
Pro Liter vernebeltem und verdunstendem Wasser werden circa 0,7 kW/h zusätzlicher Energie zur Kühlung frei. Dies liegt an der Änderung des Aggregatzustandes des Wassers. Das Wasser nimmt beim Verdampfen viel Energie auf. Bei einem Kubikmeter Wasser summiert sich die Leistung auf bereits 700 kW für eine Stunde. Ab 28 Grad Celsius schaltet dann auch die geothermische Kühlung zu. Sie kann das Datacenter auch bei Tageshöchsttemperaturen über 28 Grad kühlen.
Im Inneren des Hochbunkers kommen In-Row-Cooling-Systeme zum Einsatz. Zudem werden einige Flächen durch Betonkernaktivierung gekühlt. Bei einem ehemaligen Atombunker mit zwei Meter dicken Beton-Außenwänden bietet sich das an. Deswegen wird im Gebäude selbst die Energie mit Hilfe von Betonkernaktivierung eingespeichert und großflächig ausgetauscht.
ColocationIX kommt mit deutlich unter fünf Prozent des Stromverbrauchs für Kühlung aus und nutzt die Abwärme auch zum Heizen.

Ausblick

Für die kommende Zeit verspricht sich die Nehlsen AG durch den Colocation-Partner weitere Vorteile bei der Anbindung zusätzlicher, sowohl nationaler als auch internationaler Standorte und profitiert von der sehr guten und heutzutage immer wichtigeren Internet- sowie WAN-Anbindung des Rechenzentrums selbst. Damit passt sich der IT-Dienstleister flexibel an den wachsenden Bedarf des Entsorgers an.

Da die Wartungsarbeiten an den Infrastrukturkomponenten entfallen, können sich die IT-Mitarbeiter zudem wieder auf ihre Kernkompetenzen konzentrieren.
Dazu gehören das umfängliche Hosting sowie der Betrieb aller erforderlichen Anwendungen bei Nehlsen, der Benutzersupport, die Wartung und regelmäßige Erneuerung der Server- und Netzwerkinfrastruktur sowie IT-Projekte wie eine ERP-Ablösung und weitere kleinere Softwareprojekte. „Dabei muss niemand dafür Sorge tragen, dass die Infrastruktur nicht in sicheren Händen ist", resümiert Moje. „Eine Sorge weniger!"

Kommentar

Rekordstrafe für Google nach DSGVO-Verstoß sollte als Warnung für andere Unternehmen gesehen werden

Ein Kommentar von Dr. Guy Bunker, Senior VP of Products & Marketing bei Clearswift

Laut der im Mai 2018 verbindlich in Kraft getretenen europäischen Datenschutzgrundverordnung können die nationalen Aufsichtsbehörden Bußgelder für bestimmte Datenschutzverstöße verhängen. Für besonders gravierende Verstöße beträgt der Bußgeldrahmen bis zu 20 Millionen Euro oder im Fall eines Betriebes bis zu 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr – je nachdem, welcher Wert der höhere ist. Seit letztem Mai sind hohe Sanktionen gegen Großkonzerne bisher allerdings ausgeblieben. Im Oktober letzten Jahres war in Portugal die europaweit erste substanzielle Geldstrafe wegen eines Verstoßes gegen die Verordnung verhängt worden. Damals gab die portugiesische Datenschutzbehörde CNPD (Comissão Nacional de Protecção de Dados) bekannt, dass das Krankenhaus Barreiro Montijo unweit von Lissabon 400.000 Euro bezahlen solle. Der Hauptgrund für die behördliche Ahndung war, dass hier klinikintern zu viele Personen Zugriff auf vertrauliche Patientendaten hatten.
Wie Anfang dieser Woche berichtet wurde, muss der US-Suchmaschinenriese Google in Frankreich die erste hohe Geldbuße aufgrund von Verstößen gegen die EU-DSGVO zahlen. Konkret beläuft sich die zu zahlende Strafe auf 50 Millionen Euro. Als Grund gab die französische Datenschutzbehörde CNIL (Commission Nationale de l'Informatique et des Libertés) fehlende Transparenz an. Die Nutzer von Google seien nicht „klar und verständlich" über die Nutzung der persönlichen Daten informiert worden. Um die Informationspolitik des Konzerns gegenüber seinen Nutzern zu überprüfen, ging die CNIL schrittweise die Anmeldung eines mobilen Users des Android-Betriebssystems für die Eröffnung eines Google-Kontos durch. Bemängelt wurde unter anderem, dass Nutzer mehrere Klicks benötigen würden, um an wichtige Informationen bezüglich der Zwecke der Datenverarbeitung und der Datenspeicherungsdauer zu gelangen und diese oft auf mehrere Dokumente verteilt worden seien.
Grundlage der Bußgeld-Forderung waren zum einen die Klage der österreichischen Non-Profit-Organisation NOYB um den Datenschutzaktivist Max Schrems, und einer französischen NGO namens LQDN. Im Hinblick auf die DSGVO stellt der Fall einen der ersten in dieser Art dar – die französische Datenschutzbehörde ist die erste Kontrollinstitution, die in dieser Form einen globalen Internetkonzern abstraft.

Bei der Sanktion gegen Google in Frankreich handelt es sich im Rahmen der DSGVO um eine erhebliche Geldstrafe. Zwar stellen die 50 Millionen Euro bei weitem nicht die maximal verfügbare Buße dar, doch der Betrag reicht allemal, um andere Firmen aufhorchen zu lassen und Notiz zu nehmen. Der Fall zeigt weiterhin, dass kein Unternehmen über dem Gesetz steht und die Regulierungsbehörden künftig große, namhafte Konzerne verfolgen könnten.
Betriebe, die aufgrund der jüngsten Entwicklungen erhebliche Geldstrafen gegenüber ihrem eigenen Unternehmen befürchten, sollten sich bewusst machen, dass der Schlüssel zur DSGVO-Compliance sich auf drei zentrale Aspekte erstreckt: Menschen, Prozesse und Technologien. Dies sind die wichtigen Bereiche, welche von Firmen überprüft werden müssen, um Sichtbarkeit und Kontrolle der kritischen Daten zu erlangen und schließlich mit der Datenschutzgrundverordnung konform zu sein. Hierbei ist es essentiell, dass der Vorstand und die mittlere Führungsebene zusammenarbeiten, um ein klares Verständnis vom aktuellen Status der Datensicherheit und des Datenschutzes zu erhalten. Nur durch effektive betriebsinterne Kooperation kann ein hohes Level an Sicherheit sowie die Konformität mit der Verordnung erreicht und aufrechterhalten werden.