

# Special Sicherheit im Rechenzentrum



Die Zeitschrift für  
Informations-Sicherheit

Die optimale Luftfeuchte im  
Serverraum

Seite 1

Data Center zukunftsfit machen

Seite 4

Kopplung von Rechenzentren:  
Sicher und schnell auf Layer 2

Seite 6

## Mitherausgeber



## Impressum



Augustinusstraße 9d, 50226 Frechen (DE)  
Tel.: +49 2234 98949-30,  
Fax: +49 2234 98949-32  
redaktion@datakontext.com,  
www.datakontext.com

Geschäftsführer: Dr. Karl Ulrich

Handelsregister:  
Amtsgericht Köln, HRB 82299

Anzeigenleitung: Birgit Eckert  
(verantwortlich für den Anzeigenteil)  
Tel.: +49 6728 289003, anzeigen@kes.de

Satz: BLACK ART Werbestudio  
Stromberger Straße 43a, 55413 Weiler

Druck: QUBUS media GmbH,  
Beckstraße 10, 30457 Hannover

## RZ-Planung

# Die optimale Luftfeuchte im Serverraum

Die Luftfeuchte im Serverraum ist neben der Lufttemperatur ein entscheidendes Kriterium der Umgebungsbedingungen, das Einfluss auf Funktionalität und Lebensdauer der IT hat. Hohe Luftfeuchte führt bei entsprechenden Temperaturen zu Korrosionserscheinungen, zu niedriger Luftfeuchte kann elektrostatische Entladungen begünstigen und ebenfalls Schäden verursachen. Was sind aber optimale Werte für eine betriebssichere IT?

Von Christoph Riedel, von zur Mühlen'sche (VZM) GmbH

Spricht man von der Luftfeuchte in einem Serverraum, wird als Messgröße oft die relative Luftfeuchtigkeit herangezogen. Denn während sich der Wassergehalt als Wasserdampf in der Luft in bestimmten Grenzen unabhängig der Tem-

peratur verhält (absolute Feuchte), verändert sich die relative Luftfeuchte in Abhängigkeit der Temperatur. Je wärmer die Luft ist, desto mehr Feuchtigkeit kann sie aufnehmen, umgekehrt sinkt die Aufnahmekapazität bei fallender Temperatur.

Wie fast alles bei uns werden auch Anforderungen an Umgebungsbedingungen in einem Rechenzentrum (RZ) oder Serverraum in Normen und Regelwerken definiert. Diesbezüglich sind in erster Linie folgende Regelwerke zu nennen:

— DIN EN 50600, Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren, Teil 2-3: Regelung der Umgebungsbedingungen; von August 2019

— VDI 2054, Raumlufttechnik – Technische Anlagen zur Konditionierung von Einrichtungen für die Datenverarbeitung; von Mai 2018

— ASHRAE TC 9.9, Thermal Guidelines for Data Processing Environments, Fourth Edition (2015)

Die American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) gilt als Mutter aller RZ-Anwendungsregeln und publiziert bereits seit 2004 Vorgaben für betriebs sichere Umgebungsbedingungen in Rechenzentren. Die Reihe DIN EN 50600 nor-

miert seit etwa 2013 deutsche und europäische Rechenzentren und hat seit 2019 auch als Reihe ISO 22237 weltweite Relevanz bekommen. Die VDI 2054 fand in der Version von 1994 zuletzt keine Berücksichtigung mehr, wurde im Mai 2018 jedoch vollständig überarbeitet.

Fangen wir mit der DIN EN 50600 an: Dort sind keine konkreten Grenzwerte für die relative Luftfeuchte definiert. Sie beschreibt zwar informativ die Einhaltung solcher Grenzwerte und nennt einen Taupunkt von 5,5 Grad Celsius für alle Bereiche, in denen das Risiko der Beschädigung elektrostatisch empfindlicher Geräte besteht. Im Weiteren verweist sie jedoch auf die CLC/TR 50600-99-1, Empfohlene Praktiken

für das Energiemanagement. Dieses Werk wiederum zeigt einen Auszug aus dem ASHRAE-Klassifikationssystem mit der Empfehlung, das vollständige ASHRAE-Dokument mit den Leitlinien zurate zu ziehen. Die DIN EN 50600 verweist also bezüglich einzuhaltender Grenzwerte für Rechnerräume auf die ASHRAE.

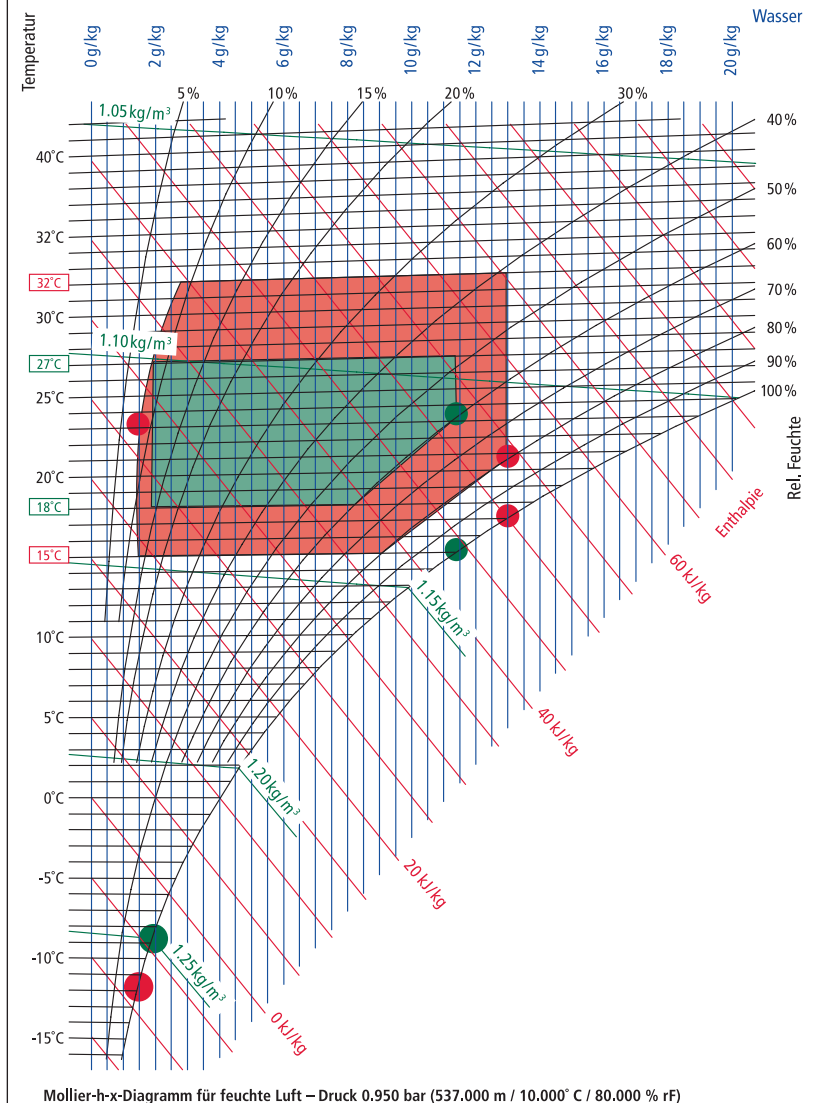
Die VDI 2054 wiederum nennt „übliche untere und obere Grenzwerte“ von 20 und 80 Prozent relativer Luftfeuchte, eine präzisere Vorgabe oder Empfehlung ist hier jedoch nicht zu finden. Vielmehr Aussagen wie: „die Untergrenze der Luftfeuchtigkeit ergibt sich aus der Vermeidung von Störeffekten durch elektrostatische Aufladung“. Als weiterführende technische Regel ist hier ebenfalls die ASHRAE aufgeführt. Die vorab genannten 20 bis 80 Prozent relative Luftfeuchte entsprechen auch nicht mehr den aktuellen Empfehlungen der ASHRAE.

### Empfehlungen der ASHRAE

Nachdem nun sowohl die DIN EN 50600 als auch die VDI 2054 auf die ASHRAE TC 9.9 verweisen, lohnt es sich, einen Blick dort hineinzuworfen. Sie definiert tatsächlich Grenzwerte für eine relative Luftfeuchte in Abhängigkeit von Geräteklassen. Unterschieden wird dabei zwischen einem empfohlenen Bereich (recommended) und einem erlaubten Bereich (allowable). Während der empfohlene Bereich für alle Geräteklassen herangezogen werden soll (A1 bis A4), sind die erlaubten Werte den einzelnen Geräteklassen zugeordnet. Für die relative Luftfeuchte nennt die ASHRAE folgende Werte:

- empfohlen (recommended, Geräteklasse A1 bis A4): 9 °C DP to 15 °C DP and 60 % RH
- erlaubt (allowable, Geräteklasse A1): 12 °C DP and 8 % RH to 17 °C DP and 80 % RH

Empfohlener und erlaubter Bereich für betriebs sichere Umgebungsbedingungen nach ASHRAE (Fourth Edition, 2015); Bild: cr/VZM GmbH



Zur Erinnerung: Die relative Feuchte ändert sich in Abhängigkeit zur Temperatur, jeder Luftzustand hängt also neben der Luftfeuchtigkeit auch von der Lufttemperatur ab. Aus der Kombination dieser Werte ergibt sich dann ein Taupunkt, an dem die Luft keine Feuchtigkeit mehr aufnehmen kann. In den oben genannten Werten ist dieser Taupunkt mit „DP“ abgekürzt (Dew Point). „RH“ wiederum steht für die relative Luftfeuchte (Relative Humidity). Die ASHRAE definiert also keine statischen Grenzwerte der relativen Luftfeuchte (z. B. 20 bis 80 Prozent), sondern nennt Taupunkte, aus denen sich in Zusammenhang mit der Temperatur Grenzen für betriebssichere Umgebungsbedingungen ableiten lassen.

Um nun diese Grenzen definieren zu können, fehlen also noch die zugehörigen Temperaturen. Auch diese sind in der ASHRAE definiert:

— empfohlen (recommended Geräteklasse A1 bis A4): 18 °C bis 27 °C

— erlaubt (allowable Geräteklasse A1): 15 °C bis 32 °C

Überträgt man nun die genannten Werte der ASHRAE (Feuchte mit den zugehörigen Temperaturen (Zuluft IT)) in ein Mollier-h-x-Diagramm (siehe Abbildung), ergeben sich Bereiche, in denen – nach Erfahrung und Empfehlung der ASHRAE – ein ideales Verhältnis zwischen einem möglichst großen Regelbereich (wirtschaftlicher Betrieb) und der Betriebssicherheit der eingesetzten IT besteht. In der Abbildung haben wir dazu die Grenzwerte farblich punktiert und daraus die zwei Bereiche abgeleitet: Der grüne Bereich entspricht den empfohlenen Werten, der rote den etwas großzügiger gefassten erlaubten Werten.

Die Einhaltung einer Luftfeuchte von acht Prozent stößt bei RZ-Verantwortlichen oft erst einmal auf Unverständnis, doch die ASHRAE

erklärt sehr genau, wie sie zu diesen Erkenntnissen kommt. Die Erläuterungen finden sich in Anhang D der ASHRAE (ESD Research and Static Control Measures). Die ASHRAE hat eigene Versuche durchgeführt, um das Risiko von Störungen oder Schäden an Elektronik im Zusammenhang mit elektrostatischer Entladung (ESD, engl. electrostatic discharge) in Rechenzentren zu untersuchen, mit dem Schwerpunkt eines erhöhten Risikos bei reduzierter Luftfeuchtigkeit. Zusammengefasst wurde festgestellt, dass bei Nutzung von ESD-abmildernden Bodenbelägen und Schuhen, wie es Standard in allen Rechenzentren sein sollte, die Gefahr von ESD-Störungen auf ein unbedeutendes Maß reduziert werden kann – auch wenn die Luftfeuchtigkeit auf sehr niedrige Werte, zum Beispiel acht Prozent, eingestellt wird. Bei Arbeiten an besonders empfindlichen internen Bauteilen der IT, wie den Motherboards oder Central Processing Units (CPUs), sind in diesem Fall jedoch zusätzliche ESD-Schutzmaßnahmen nötig, wenn diese im Serverraum durchgeführt werden. Ansonsten können bei Einhaltung dieser Werte und der üblichen ESD-Schutzstandards die bekannten Probleme der Betriebssicherheit und Verfügbarkeit der IT aufgrund zu geringer oder zu hoher Luftfeuchte vermieden werden.

Welcher Bereich jedoch genau einzuhalten ist, beispielsweise ob der empfohlene oder der erlaubte nach ASHRAE, ist idealerweise bereits in der Planungsphase gemeinsam mit dem RZ- oder Serverraum-Verantwortlichen festzulegen. Neben wirtschaftlichen Aspekten sollten dazu auch die Ergebnisse einer Geschäftsrisikoanalyse (Verfügbarkeitsanforderungen) ausschlaggebend sein.

## Fazit

Weder die DIN EN 50600-2-3 noch die VDI 2054, machen konkrete Vorgaben für die Luftfeuchte

in Rechnerräumen. Grenzwerte finden sich lediglich in der ASHRAE, und die dort definierten Werte der relativen Luftfeuchte ergeben nur im Zusammenhang mit den einzuhaltenden Lufttemperaturen ein Bild. Die ASHRAE TC 9.9 gibt RZ-Betreibern und Verantwortlichen für das Facility Management oder die Gebäudeautomation also großzügige Werte an die Hand, mit denen sich ein betriebssicherer und energieeffizienter Betrieb der IT umsetzen lässt. Es ist Aufgabe der Planungs- oder Betriebsverantwortlichen, daraus konkrete Vorgaben für den Betrieb der raumlufttechnischen Anlagen abzuleiten. ■

Durch IT- und Infrastruktur-Lösungen aus einer Hand werden Rechenzentren intelligenter, effizienter, stabiler und nachhaltiger

## Data Center zukunftsfit machen

In unserer zunehmend vernetzten Welt steigt die Datenmenge überproportional stark an. Außerdem sind Organisationen aller Größenordnungen und Branchen heute auf die ständige Verfügbarkeit ihrer Daten angewiesen – rund um die Uhr den Zugriff auf Big Data und das Internet of Things zu haben ist zu einer geschäftskritischen Anforderung geworden. Schon der kurze Ausfall eines Rechenzentrums kann massive wirtschaftliche Auswirkungen nach sich ziehen. Störungen lassen sich mit moderner IT und Infrastruktur jedoch vorbeugen: Data Center, die fit für die Zukunft sind, arbeiten stabiler, sicherer und darüber hinaus auch effizienter und nachhaltiger.

Von Malte Gloth, Johnson Controls



Rechenzentren, die umfassende Datenvolumen beherbergen und den Nutzern an 365 Tagen im Jahr unterbrechungsfrei zur Verfügung stehen, sind heute zu kritischen Schnittstellen geworden. (Bild: Johnson Controls)

Während die ständige Verfügbarkeit der Daten, deren Sicherheit sowie die Wirtschaftlichkeit des Betriebs lange zu den grundlegenden Anforderungen an ein Rechenzentrum (RZ) zählen, rückt in den letzten Jahren der Umweltaspekt zunehmend in den Mittelpunkt – und das nicht erst, seitdem die Bundesregierung die Klimaneutralität bis 2045 mit ihrem Klimaschutzgesetz 2021 obligatorisch gemacht hat.

Rechenzentren gehören seit jeher zu den größten Stromverbrau-

chern: In Europa ist ihr Energiebedarf laut dem Borderstep Institut für Innovation und Nachhaltigkeit zwischen 2010 und 2020 um etwa 55 Prozent auf rund 87 Terrawattstunden pro Jahr gestiegen. Speziell für Deutschland sagte das Institut 2015 gemeinsam mit dem Berliner Fraunhofer-Institut IZM voraus, dass der Energiebedarf der Rechenzentren bis 2025 noch auf über 25 Terrawattstunden zunimmt. Dieser stark ansteigende Stromverbrauch führt zwangsläufig zu mehr umweltschädlichen Emissionen, sofern die Energiebilanz der Rechenzentren nicht gleichzeitig mithilfe einer State-of-the-Art-Infrastruktur optimiert wird.

### 360-Grad-Lösungen ebnen den Weg zur Klimaneutralität

Für die Energieeffizienz eines Rechenzentrums wird der Power-Usage-Effectiveness-(PUE)-Wert als Kenngröße verwendet. Er gibt Aufschluss darüber, wie effektiv ein Rechenzentrum die ihm zugeführte Energie verbraucht. Bei der Berechnung wird die zugeführte Energie durch die vom Equipment verbrauchte Energie geteilt: Je näher

sich der ermittelte Wert an die 1,0 annähert, desto energieeffizienter arbeitet das Rechenzentrum und desto besser ist seine Energiebilanz. Sparsame Data Center haben demnach einen PUE-Wert von 1,2 bis 1,3 oder niedriger.

Bei der Optimierung des PUE-Wertes unterstützt Johnson Controls: Sein 360-Grad-Portfolio für Rechenzentren umfasst digitale sowie physische Lösungen für Energie- und Gebäudemanagement, Brandschutz und Gebäudeüberwachung. Alle Produkte ([www.johnsoncontrols.com/de\\_de/branchen/rechenzentren](http://www.johnsoncontrols.com/de_de/branchen/rechenzentren)) sind in der neuen digitalen Plattform OpenBlue gebündelt. Sie lässt die Einzelgewerke nahtlos ineinandergreifen und führt alle relevanten Daten und Informationen aus verschiedenen Systemen zusammen.

In einem Data Center integriert OpenBlue übergreifend das Facility- und IT-Management von Gebäuden und erlaubt die Kontrolle und Automatisierung der gesamten Infrastruktur. Dabei bindet die intelligente Architektur auch die Systeme, Lösungen und Komponenten fremder Technologie-Anbieter prob-

lemlos ein und erlaubt so die Überwachung und Steuerung heterogener Systemlandschaften. Die Energieeffizienz und entsprechend die Kohlenstoffemissionen lassen sich mit OpenBlue um 50 Prozent und mehr verbessern.

Das professionelle Management komplexer Abläufe und Prozesse durch OpenBlue optimiert das Zusammenspiel der verschiedenen Einzelkomponenten im Rechenzentrum – und führt insgesamt zu deutlich mehr Stabilität, Sicherheit und Energieeffizienz. Ebenso sinkt der PUE-Wert und Betreiber können sich schneller ihrem Netto-Null-Emissionen-Ziel nähern. Johnson Controls selbst hat sich bereits bis 2040 zur Netto-Null verpflichtet und kündigt wissenschaftlich fundierte Ziele für 2030 an.

## Ein Anbieter für alle Gewerke bietet viele Vorteile

Nicht allein mit OpenBlue, sondern auch mit integrierten Soft- und Hardware-Lösungen, etwa aus den Bereichen Klimatisierung, Brandschutz und Sicherheit, begleitet Johnson Controls Rechenzentren in all ihren Lebenszyklus-Phasen. Die zahlreichen Lösungen aus einer Hand interagieren maximal effizient miteinander und Betreiber haben dafür komfortabel nur einen zentralen Ansprechpartner, was ihnen zusätzlich Zeit und Geld einspart.

Außerdem ist die Infrastruktur eines Data Centers durch die Bündelung der Kompetenz bei nur einem Anbieter leichter skalierbar. Dies spielt eine große Rolle, denn dem rasanten Datenwachstum muss sich nicht nur das IT-Umfeld, sondern die gesamte Infrastruktur eines Rechenzentrums anpassen können. Zum Beispiel müssen die Anlagen für die Kälte- und Stromversorgung mitwachsen. Sie sind wesentlich für den unterbrechungsfreien Betrieb, können aber nicht im selben Tempo

erneuert oder erweitert werden wie IT-Komponenten, weil sie einen längeren Lebenszyklus haben. An dieser Stelle braucht es ganzheitliche Ansätze, in deren Erarbeitung Johnson Controls über 136 Jahre Erfahrung hat.

## Klimatisierung, Stromversorgung, Brandschutz und physische Sicherheit

Innerhalb von OpenBlue ist das Gebäudemanagementsystem Metasys verantwortlich für die Analyse, Auswertung und Visualisierung aller zusammenfließenden Daten. Es regelt beispielsweise die Heizungs-, Lüftungs- und Klimatechnik. Um schlankeren und leistungsfähigeren Servern, die mehr Strom benötigen und dadurch mehr Wärme erzeugen, weiter Herr zu werden, ist eine immer leistungsstärkere Kühlung für die Technik nötig. OpenBlue verhindert, dass die Server im Rechenzentrum überhitzen, erkennt Störungen automatisch und alarmiert falls nötig die Betreiber.

Neben der Klimatisierung ist die wohl grundlegendste Voraussetzung für den stabilen Betrieb des Rechenzentrums die Stromversorgung. Diese wird redundant ausgelegt und um unterbrechungsfreie Stromversorgungs-Anlagen (USV) und Generatoren ergänzt. Im laufenden Betrieb übernimmt OpenBlue dann die ständige Überwachung der Stromversorgung, kontrolliert den Verbrauch sowie die Versorgungsqualität und stellt die hohe Verfügbarkeit sicher. Weichen Messwerte ab, wird auch hier frühzeitig ein Alarm ausgelöst.

In Rechenzentren ist überdies Feuer eine der häufigsten Ursachen für Betriebsausfälle. Um Daten, Hardware und Mitarbeiter zu schützen, muss das Brandrisiko minimiert werden. Auch hier bietet Johnson Controls Lösungen an, stets mit dem Ziel, entstehende Brände möglichst früh zu erkennen und



Johnson Controls begleitet Rechenzentren in allen Lebenszyklus-Phasen. Das Portfolio umfasst digitale und physische Lösungen für Energie- und Gebäudemanagement, Brandschutz und Gebäudeüberwachung. Sie werden gebündelt in der digitalen Dach-Architektur OpenBlue. (Bild: Johnson Controls)

wirkungsvoll zu bekämpfen. Zum Beispiel gibt es Ansaugrauch- und Brandmelder für die Rechnerräume, die permanent Luftproben nehmen und auf Rauchpartikel untersuchen. Im Brandfall können automatisch Gaslöschsysteme ausgelöst werden, die den Serverraum nach vorheriger Evakuierung zeitnah mit Stickstoff oder Argon fluten. Sie löschen das Rechenzentrum – anders als Wasser oder Schaum – rückstandslos.

Ebenfalls Teil des Portfolios von Johnson Controls für Rechenzentren und Gebäude aller Art sind Komponenten für die physische Sicherheit. Während der Gesetzgeber beim Brandschutz Vorgaben macht, definieren Unternehmen hinsichtlich Zutrittskontrolle und (IT-)Sicherheit individuelle Standards. Sie können etwa Systeme für die Zutrittsberechtigung, den Einbruchschutz oder die Videoüberwachung der Innen- und Außenbereiche umfassen. Johnson Controls bietet diese Lösungen an, die auch selbst optimal vor Hackern und Cyberkriminellen geschützt sind. Damit stellt der Experte in allen Dimensionen sicher, dass ein Rechenzentrum reibungslos betrieben werden kann. ■

Malte Gloth ist seit Juni 2021 Head of Key Account Management, Verticals and Digital Solutions Germany bei Johnson Controls.

# Kopplung von Rechenzentren: Sicher und schnell auf Layer 2

Heute müssen Unternehmen und Behörden immer mehr sensible Daten über öffentliche Leitungswege austauschen, zum Beispiel wenn sie Rechenzentren miteinander koppeln, um Daten in Echtzeit spiegeln zu können. Die SINA L2 Boxen gewährleisten auf Netzwerkschicht 2 einen sicheren und schnellen Informationsaustausch durch Ethernet-Verschlüsselung.

Von Linda Leffler, secunet Security Networks AG

Digitalisierung, Automatisierung, Cloud Computing und Big Data fordern uns nicht nur fachlich mehr ab, sondern auch technisch. Eine entscheidende Rolle spielt dabei die Datenübertragung. Immer mehr Unternehmen benötigen erhöhten Datendurchsatz bei geringer Latenz. Bei der Vernetzung von Standorten oder der Nutzung cloudbasierter Anwendungen steigen die Anforderungen beispielsweise schnell in den Bereich von bis zu 100 Gbit/s. Ein weiteres Szenario mit sehr hohem Bandbreitenbedarf ist die Kopplung von Rechenzentren, zum Beispiel bei einer redundanten Implementierung, bei der ein Rechenzentrum als Backup für ein anderes dient und Daten in Echtzeit gespiegelt werden müssen.

Sind in solchen Anwendungsfällen sensible oder gar eingestufte Daten im Spiel, muss die Datenübertragung angemessen verschlüsselt werden. Für dieses Szenario sind andere Krypto-Lösungen gefragt als bei der Anbindung von einzelnen Endgeräten via VPN, bei denen typischerweise auf Layer 3 über das IPsec-Protokoll verschlüsselt wird. Entscheidend für den Durchsatz ist die Netzwerkschicht.

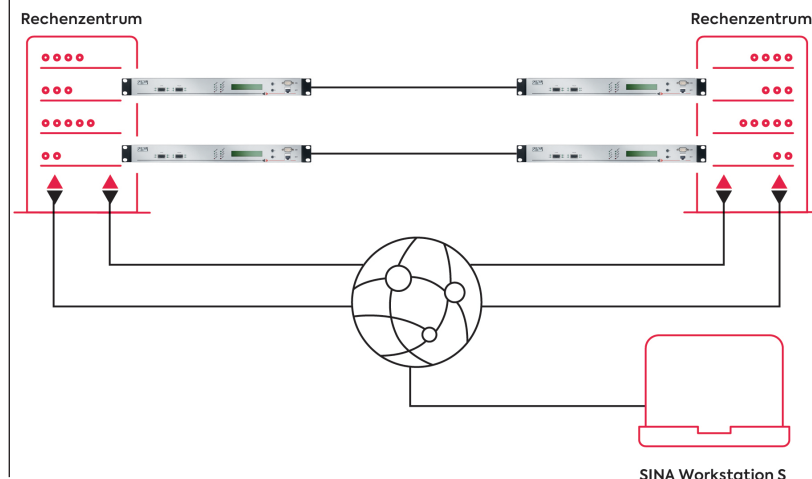
Das OSI-Modell ist als Standardreferenz für die Schichtenarchitektur der Netzwerkprotokolle definiert. Die sieben aufeinander aufbauenden Schichten (Layer) sind mit spezifischen Aufgaben assoziiert. So beschreibt die unterste Schicht (L1) eine Verbindung auf der physischen

Ebene, zum Beispiel als Bitstrom bei einem Wavelength-Division-Multiplexing-(WDM)-System, die zweite zum Beispiel eine Ethernet-Verbindung (L2), die dritte beispielsweise eine IP-Verbindung (L3). Je nach Bedarf der Applikationsumgebungen eignen sich vor allem L2- oder L3-basierte Lösungen für verschiedene Einsatzbereiche der verschlüsselten Datenübertragung. So haben etwa L3-basierte Lösungen Flexibilität- und Skalierungsvorteile, wenn eine hohe Anzahl von Endpunkten mit jeweils kleinem Bandbreitenbedarf besteht und eine L2-Anschlussmöglichkeit fehlt, zum Beispiel VoIP-Endpunkte oder mobile Zugänge.

## Verschlüsselung auf der Ethernet-Schicht

Für die sichere Kopplung von Rechenzentren oder die Kopplung eines Hauptstandorts mit mehreren Nebenstandorten bieten sich Layer-2-Verbindungen mit entsprechend sicherer Verschlüsselung an. Denn bei einer geringen bis mittleren Anzahl von Endpunkten (meist weniger als 100) mit größerer Bandbreite (mehr als 1 Gbit/s) sowie weitestgehend symmetrischen Topologien haben Layer-2-basierte Krypto-Lösungen deutliche Effizienz- und Kostenvorteile hinsichtlich der Datenübertragung. In Summe wird über alle Verbindungen weniger Overhead, also zusätzliche Daten, erzeugt und die zur Verfügung gestellt

Mit der SINA L2 Box lassen sich große Datenmengen schnell und sicher zwischen Rechenzentren übertragen.



hende Bandbreite besonders effizient genutzt.

Zudem sind L2-Verschlüsseler transparent für die IP-Ebene (Layer 3). Dadurch behalten die Endanwender die volle Kontrolle über die IP-basierte Paketweiterleitung (Routing). Folglich erübrigt es sich, IP-Verbindungen einzeln zu verschlüsseln und Sicherheitsbeziehungen kleinteilig zu betrachten. Außerdem können Nutzer zusätzliche Routing- oder Forwarding-Technologien implementieren. Dank dieser Voraussetzungen ist es IT-Verantwortlichen möglich, sichere Kommunikation mit hohem Datendurchsatz zu gewährleisten.

Im Behördenumfeld sollen oft auch Daten übertragen werden, die als VS-NfD (Verschlusssache – Nur für den Dienstgebrauch) eingestuft sind. Dann müssen zwingend Layer-2-Verschlüsselungslösungen eingesetzt werden, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für diese Geheimhaltungsstufe zugelassen sind.

## L2-Verschlüsselungen mit bis zu 100 Gbit/s

Aus technischen Gründen waren VS-NfD-zugelassene L2-Krypto-Lösungen lange Zeit auf 40 Gbit/s beschränkt. Erhöhter Datendurchsatz ließ sich oft nur über parallel eingesetzte Systeme umsetzen. Das wiederum sorgt für erhöhten Platz- und Energiebedarf im Rack. Im Jahr 2020 hat secunet eine leistungsfähigere und dennoch für den Geheimhaltungsgrad VS-NfD zugelassene Version der SINA L2 Box S vorgestellt. Sie liefert eine Verschlüsselungsleistung von bis zu 100 Gbit/s pro Höheneinheit und begegnet damit dem erhöhten Bedarf nach Skalierbarkeit und Sicherheit im anhaltenden digitalen Transformationsprozess.

Mit der SINA L2 Box S 100G lassen sich sichere VS-NfD-konforme L2-Punkt-zu-Punkt- sowie Multipunktverbindungen aufbauen.

Die entsprechenden Applikationen können dabei in und zwischen den Rechenzentren auf L2- und L3-Ebene sicher kommunizieren. Am Zugang zum Rechenzentrum werden von der SINA L2 Box S 100G auch noch bei einer Datenrate von 100 Gbit/s nur authentifizierte Ethernet-Frames durchgelassen, ungültige hingegen hardwarebasiert verworfen. So helfen sie auch dabei, bestehende Bandbreiten effizient zu nutzen, was insbesondere im Umfeld hochverfügbarer Rechenzentrumscluster wichtig ist.

Ein weiteres wichtiges Einsatzfeld ist unter anderem die Verschlüsselung von Daten, die über WDM-Verbindungen übertragen werden. Gelegentlich setzen IT-Verantwortliche dabei auf L1-Krypto-Lösungen. Diese sind in der Regel aber nicht für VS-NfD zugelassen. Außerdem können Anwender mit ihnen nicht zwischen der Verantwortung für die Datenübertragung und jener für die Datensicherheit trennen. Zudem sind sie auf direkte Punkt-zu-Punkt-Leitungen zwischen ihren Standorten angewiesen, während L2- und L3-Verschlüsselung beliebige Zwischenstationen (Hops) im Weitverkehrsnetz und Mehrpunkt-Verbindungen erlauben.

Die SINA L2 Box S 100G verfügt über zwei Leistungsstufen, wobei das Basissystem mit 50 Gbit/s flexibel per Update auf 100 Gbit/s erweitert werden kann. So können Anwender ohne Systemwechsel zu einem späteren Zeitpunkt unkompliziert erhöhte Krypto-Durchsätze mit weiteren, kompatiblen Geräten realisieren – und dies sogar ohne Hardware-Änderung, da das Modell per Lizenz-Upgrade rein softwaremäßig und remote beschleunigt werden kann.

## Zukunftssichere Informationssicherheit

Die L2-basierte Krypto-Lösung von secunet folgt darüber

hinaus der BSI-Handlungsempfehlung zur „Migration zu Post-Quanten-Kryptografie“. Zwar ist bisher noch kein Quantencomputer verfügbar, der zum Entschlüsseln derzeit gängiger kryptografischer Verfahren geeignet wäre. Doch das wird sich künftig ändern. Und manche heute übertragenen Daten sollen auf Dekaden hinaus vertraulich bleiben, bis weit in das Post-Quanten-Zeitalter hinein. Daher ist es ratsam, schon heute präventiv Verfahren einzusetzen, die zukünftigen Angriffen leistungsfähiger Quantencomputer standhalten können.

Entsprechend der vom BSI beschriebenen potenziellen Schutzmaßnahmen ermöglicht es die SINA L2 Box S, den asymmetrischen Schlüsselaustausch zwischen zwei Geräten mithilfe eines verteilten Geheimnisses symmetrisch zu codieren. Außerdem können bei Kryptografie mit elliptischen Kurven die Kurvenparameter geheim gehalten werden, was den Angriffsvektor für potenzielle Quantencomputer-Angriffe verringert. Auf diese Weise sind Nutzer bereits jetzt auf das vorbereitet, was erst noch kommen wird. Der Zukunft einen Schritt voraus zu sein, ist schließlich eine essenzielle Leitidee im Umfeld der IT-Sicherheit. ■



# Nachhaltige und zukunftsfähige Rechenzentren mit einer ganzheitlichen Lösung von Johnson Controls

Mit der zunehmenden Datenverarbeitung steigen auch die Anforderungen an die Infrastrukturen von Rechenzentren. Um einen reibungslosen Betriebsablauf ohne Ausfälle der physikalischen Sicherheit und IT sicherzustellen, muss die Gebäudeinfrastruktur widerstandsfähig und gegen Gefahren wie Brände, Überhitzung oder Cyber-Angriffen gesichert sein. Erreichen Sie durch ein integriertes Managementsystem, welches Ihre Gebäudeinfrastruktur zentral überwacht und steuert, einen zuverlässigen und sicheren Betrieb – während gleichzeitig die Betriebskosten und CO<sub>2</sub>-Emission reduziert werden.

Profitieren Sie dabei von unserer 135-jährigen Erfahrung in der Gebäudetechnik mit modernster Technologie.



Weitere Informationen finden Sie unter [www.johnsoncontrols.de](http://www.johnsoncontrols.de)

The power behind **your mission**

