

30 YEARS
ANNIVERSARY

techconsult
TECHNOLOGY MARKET ANALYSTS

Modernes Netzwerkmanagement

Mit skalierbaren und Cloud-nativen Lösungen
zur ganzheitlichen Netzwerkkontrolle

Unterstützt durch

LANCOM
SYSTEMS

Inhalt

Einleitung	2
Netzwerkmanagement der Unternehmen	3
Stolpersteine des Netzwerkmanagements	4
USP: Netzwerkmanagement aus der Cloud	6
Fazit	9
Studiensteckbrief	10
Weitere Informationen	11

Einleitung

Homeoffice und COVID-Pandemie haben die Digitalisierung in den letzten 2 Jahren in den Unternehmen noch weiter angefacht. Cloud-Infrastrukturen sind in den Fokus gerückt worden und neue Software-definierte-Lösungen wurden in IT-Bereichen etabliert, die zuvor hardwareseitig für Probleme gesorgt haben. Sie sollen nun die Unternehmen dabei unterstützen, den immer größer werdenden Erwartungen gerecht zu werden. Vor allem im Netzwerkmanagement ist ein Wandel zu erkennen. Unternehmen müssen in der Lage sein, ihre Netzwerke flexibel an neue Leistungsanforderungen anzupassen. Generell spielen Flexibilität und Skalierbarkeit in der heutigen Zeit eine viel größere Rolle als noch vor einigen Jahren. Zusätzlich haben sich nicht nur die Arbeitsweisen und Techniken gewandelt. Auch die Anzahl der Geräte in den Netzwerken ist rasant gestiegen.

Diese gilt es nun zu identifizieren, zu verwalten und zu verbinden. Das ist nicht immer leicht, denn jedes Gerät bringt verschiedene Eigenschaften, Funktionen und Sicherheitsrisiken mit sich. Dort den Überblick behalten zu können, bereitet oftmals den Netzwerkadministratoren unruhige Tage. Doch automatisierte und performante Netzwerke sind mittlerweile Voraussetzung für moderne Digitalisierungstechnologien (wie z. B. IOT oder Multi-Cloud).

Doch wie sieht die aktuelle Situation hinsichtlich Netzwerkmanagement in den Unternehmen aus? Mit welchen Herausforderungen haben Anwender zu kämpfen? Welche Vorteile bietet das Netzwerkmanagement? Und was bringt eine Migration in die Cloud? Diese und weitere Fragen werden in der Studie „Modernes Netzwerkmanagement“ untersucht und vorgestellt. Als Datenbasis dienen die Antworten von 200 IT-Experten aus 200 Unternehmen ab 150 und bis 2500 Beschäftigten.

Copyright

Diese Studie wurde von der techconsult GmbH verfasst und von der LANCOM Systems GmbH unterstützt. Die darin enthaltenen Daten und Informationen wurden gewissenhaft und mit größtmöglicher Sorgfalt nach wissenschaftlichen Grundsätzen ermittelt. Für deren Vollständigkeit und Richtigkeit kann jedoch keine Garantie übernommen werden. Alle Rechte am Inhalt dieser Studie liegen bei der techconsult GmbH. Vervielfältigungen, auch auszugsweise, sind nur mit schriftlicher Genehmigung der techconsult GmbH gestattet.

Disclaimer

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen etc. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. In dieser Studie gemachte Referenzen zu irgendeinem spezifischen kommerziellen Produkt, Prozess oder Service durch Markennamen, Handelsmarken, Herstellerbezeichnung etc. bedeuten in keiner Weise eine Bevorzugung durch die techconsult GmbH.

Netzwerkmanagement der Unternehmen

Globalisierung, Digitalisierung und Pandemie haben den Unternehmen gezeigt, dass die technischen Voraussetzungen für eine zukunftssichere Arbeitsweise noch nicht vollkommen ausgereift sind. Dabei ist nicht nur die Anzahl, sondern auch die Variation der Geräte im Netzwerk allein schon durch Homeoffice rasant gestiegen. Dies wirkt sich auch auf die Netzwerksicherheit aus. Es sind nicht mehr nur definierte und bekannte Geräte wie Arbeitsrechner und Laptops zu verwalten. Viele meist kleinere Geräte finden sich nun ebenfalls im Netzwerk wieder. Eine Netzwerkarchitektur hat mittlerweile eine Vielzahl an Sensoren, Reglern, Routern, Switches und Access Points im Einsatz. Hinzu kommt die Standortvernetzung, die im Zuge der Globalisierung, Internationalisierung sowie dem Auslagern als auch dem Eingliedern von Unternehmensbereichen ein erheblicher Einflussfaktor auf die effiziente Arbeitsweise des gesamten Unternehmens geworden ist. Was es braucht, sind Netzwerkmanagementlösungen, die diese Komponenten intelligent organisieren, optimieren sowie verwalten und dem Netzwerk einen ganzheitlichen Sicherheitsstandard ermöglichen. Wichtig ist hierbei, dass sich die Unternehmen sowohl um den schnellen, zuverlässigen und kostengünstigen Datenverkehr zwischen den Standorten kümmern, als auch für ein leistungsfähiges Netzwerk vor Ort sorgen können. Unterstützung leisten dabei Technologien wie SD-WAN, SD-Branch und Firewalls.

Eine weitere Entwicklung der letzten Jahre ist der Umstieg auf die Cloud. Viele Unternehmen haben sich mittlerweile von On-Premises-Lösungen abgewandt und ihr System in die Cloud migriert. Vor allem Sicherheit, Flexibilität und Kostenkontrolle bieten Cloud-Modelle den Unternehmen an. Entsprechend hoch ist auch der Bedarf für Cloud-Lösungen im Bereich des Netzwerkmanagements zu verzeichnen.

Nur ein Viertel der befragten Unternehmen (27 Prozent) geben an, dass sie noch auf reine On-Premises-Lösungen im Bereich des Netzwerkmanagements setzen. Der Gros und damit jedes zweite Unternehmen (52 Prozent) nutzt ein hybrides System aus Cloud- und On-Premises-Lösungen. Jedes vierte Unternehmen (21 Prozent) nutzt bereits eine reine Cloud-Lösung für das Netzwerkmanagement.

Wiegen die Unternehmen alle Aspekte beider Deployment-Modelle gegeneinander auf, so zeigen sich verschiedene Vor- und Nachteile. Im On-Premises-Einsatzszenario hat die Unternehmens-IT die Lösung auf das Unternehmen angepasst sowie die volle Kontrolle über Hardware, Security und Upgrades. Damit ist die Lösung einerseits an die Anforderungen des Unternehmens ausgerichtet und andererseits an die IT-Abteilung im Unternehmen gebunden. Doch Letzteres birgt das Risiko: Die Unternehmens-IT hat in der heutigen Zeit nicht die Kapazitäten und Ressourcen, um Lösungen eigenständig zu verwalten und weiterzuentwickeln. Damit binden die Unternehmen wertvolle und besonders knappe Ressourcen an Verwaltungs- und Monitoring-Aufgaben, die vereinfacht und automatisiert werden können. Und hier treten Cloud-Lösungen fürs Netzwerkmanagement in den Fokus. Mit Hilfe von spezialisierten Anbietern im Bereich Netzwerk-Lösungen können Unternehmen eine Geschwindigkeit und einen Funktionsumfang realisieren, die sonst kosten- und zeitintensiv selbst geleistet werden müssten. Zudem garantieren die Anbieter den Betrieb, die Aktualität und die Sicherheit der Lösung. Hierdurch werden die eingangs erwähnten Herausforderungen der Flexibilität und Skalierbarkeit auch im Netzwerkmanagement abgedeckt. Doch noch weitere Herausforderungen lauern in den Netzwerken der Unternehmen.

Deployment-Modelle von Netzwerkmanagementlösungen

Basis: 200 Unternehmen



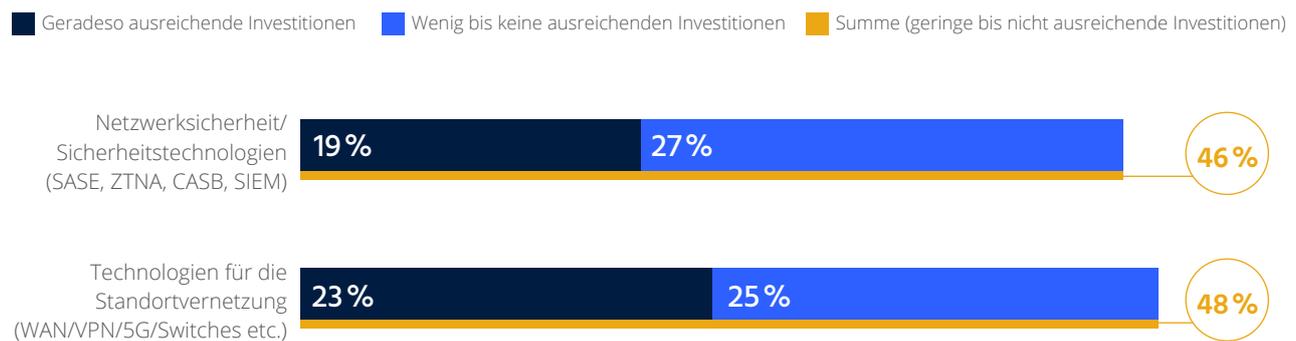
Stolpersteine des Netzwerkmanagements

Die in den Unternehmen vorhandenen Netzwerke haben sich in den letzten Jahren in ihrer Art und Architektur stark gewandelt. Es gibt nicht nur deutlich mehr, sondern auch eine Vielzahl an neuen Technologien, die es zu berücksichtigen gilt. Unter anderem kommen Cloudanwendungen und Multi-Cloud-Szenarien zum Einsatz. Damit werden neue Technologien zu potenziellen Gefahren für das Netzwerk. Intelligentes Netzwerkmanagement muss also erkennen, steuern und filtern können, wenn neue Komponente ins Netzwerk hinzukommen. Der Aspekt der Sicherheit stellt bei den befragten Unternehmen die wesentliche Herausforderung dar.

Mehr als jedes zweite Unternehmen (52 Prozent) konstatiert Probleme im Bereich der Netzwerksicherheit. Nicht verwunderlich, wenn die Unternehmen ihre Maßnahmen und Investitionen in Netzwerktechnologien reflektieren. In allen Aspekten des Netzwerkmanagements kann in Summe eine geringe bis nicht ausreichende Investitionsquote bei jedem zweiten Unternehmen festgestellt werden. Damit hängen Herausforderungen mit den mangelnden Maßnahmen und Investitionen stark zusammen.

Investitionen der Unternehmen ins Netzwerkmanagement

Basis: 200 Unternehmen



Ein weiterer Aspekt, welcher den Unternehmen Sorgen bereitet, ist der IT-Fachkräftemangel. Der Digitalisierungsdruck wächst und damit die Netzwerke der digitalen Nomaden. Neue Technologien und Geschäftsmodelle benötigen fachkundiges IT-Personal, das sich aber hauptsächlich um die wachsende Netzwerksicherheit und -verwaltung kümmern muss. Folglich bleibt oft nur wenig Zeit für neue Projekte oder Vorhaben. Damit stellt auch hier jedes zweite Unternehmen (51 Prozent) fest, dass der IT-Fachkräftemangel eine wesentliche Herausforderung innerhalb des Netzwerkmanagements darstellt.

Hinzu kommt der Aspekt der Störungssuche bzw. der Fehlerbehebung. Aufgrund der Komplexität und Größe eines Netzwerks kann es häufiger zu Fehlern und Problemen kommen. Dann gilt es, die Probleme schnellstmöglich zu beheben. Während der Behebung ist das Netzwerk jedoch nicht voll einsatzfähig und hochanfällig für Sicherheitslücken. Dies macht eine schnelle Fehlerbehebung umso wichtiger, um Ausfallzeiten zu vermeiden und die Stabilität wiederherzustellen. Gleichzeitig kann dies nicht nur einzelne Standorte, sondern das gesamte Unternehmensnetzwerk betreffen. Mit längeren Ausfällen bei der Netzwerkfehlerbehebung kämpfen knapp ein Drittel der befragten Unternehmen (32 Prozent).

Ähnlich viele Unternehmen haben Probleme mit fehlender Automatisierung. 31 Prozent der befragten Unternehmen beklagen mangelhafte bis fehlende Netzwerkautomatisierung. Das heißt, dass Unternehmen noch zu häufig Prozesse des Netzwerkmanagements manuell durchführen müssen.

Dies kann zum Beispiel die Kategorisierung eines Gerätes oder die Netzwerkdokumentation sein. Doch manuelle Prozesse erfordern Zeit und personelle Ressourcen. Aufgrund der vielfältigen neuen Technologien und Aufgabebereiche, die sich von Jahr zu Jahr wandeln, stellt Zeit und Personal die kostbarsten Ressourcen der Unternehmen dar.

Investitionen der Unternehmen in die Netzwerkautomatisierung

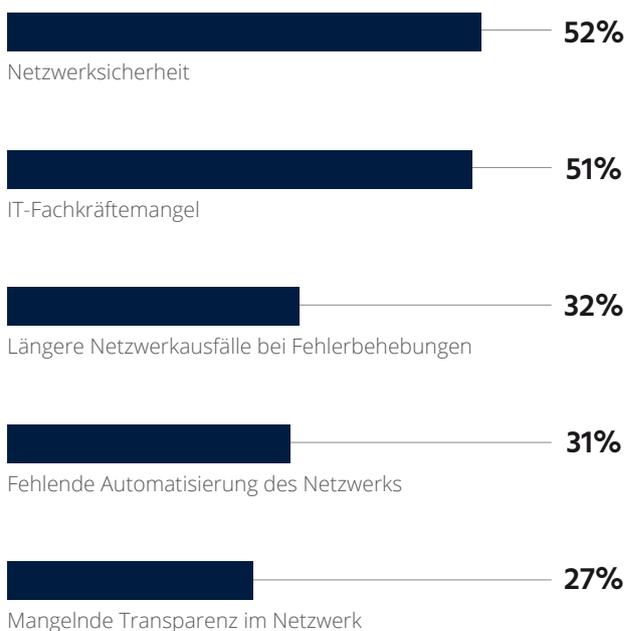
Basis: 200 Unternehmen



Sowohl für Prozesse wie des Troubleshootings oder der Netzwerkdokumentation ist eine gewisse Netzwerktransparenz vorausgesetzt. Ohne diese kann der Überblick schnell verloren gehen. Dabei sorgt die Netzwerktransparenz dafür, dass die Verantwortlichen den Überblick über eingesetzte Tools und Latenzen behalten. Verursacher für mangelnde Transparenz sind meist Insellösungen oder redundante Lösungen. Durch überschneidende Aufgabengebiete wird dann die Netzwerksicherheit gefährdet und der Zeitaufwand sowie die Kosten immens gesteigert. Hierbei klagen mehr als ein Viertel der befragten Unternehmen (27 Prozent) über mangelnde Netzwerktransparenz in ihrem Netzwerkmanagement.

Herausforderungen der Unternehmen innerhalb ihrer Netzwerke

Basis: 200 Unternehmen | Mehrfachnennungen



USP: Netzwerkmanagement aus der Cloud

Doch wie sieht der Blick in die Zukunft aus? Wie in den vergangenen Jahren zu beobachten, werden Faktoren wie Geräteanzahl, Technologien, Herausforderungen und nötiges IT-Fachwissen immer weiter ansteigen. Damit steigen auch die Anforderungen an die Netzwerke. Unternehmen müssen im Netzwerkmanagement handeln, um mit der voranschreitenden Digitalisierung mithalten zu können.

Jedes dritte Unternehmen hat mehr als 100 Netzwerkgeräte zu verwalten. Ab 1.000 Beschäftigten ist es bereits jedes zweite Unternehmen.

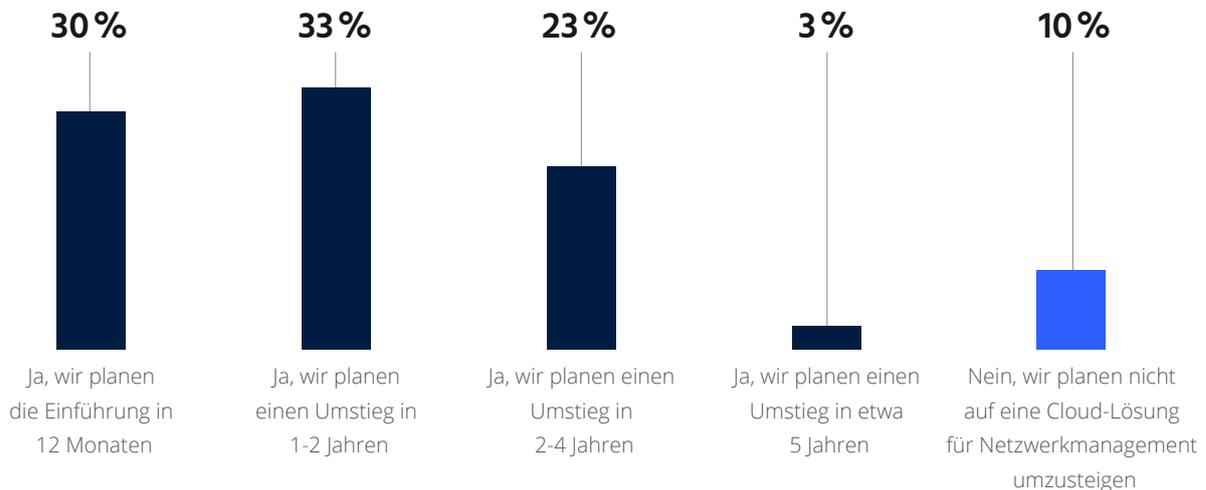
Wenn es um die Zukunft geht, geht es auch um die Cloud. Eine Migration von On-Premises zu Cloud ermöglicht den Unternehmen neue Möglichkeiten, um schneller, kostengünstiger, flexibler und skalierbarer zu sein.

Außerdem bietet sie Platz für neue Technologien wie Machine Learning und Prozessautomatisierung. Zudem lassen sich innerhalb einer Cloud-Lösung die Steuerung und der Zugriff auf Netzwerke von überall und jederzeit realisieren. Denn das Netzwerkmanagement liegt mit all seinen Bestandteilen in der Cloud und benötigt nur einen Internetzugang. Sind die Netzwerkkomponenten ebenfalls mit dem Internet verbunden, kann die Lösung darauf zugreifen und das moderne Netzwerkmanagement ist nicht mehr standortgebunden.

Dies sieht auch ein Großteil der befragten Unternehmen so. Die große Mehrheit gibt mit 85 Prozent an, einen Umstieg auf eine Cloud-Lösung in den kommenden vier Jahren anzustreben. Damit planen auch viele der Unternehmen, die momentan noch auf Hybride- und On-Premises-Lösungen zurückgreifen, den ganzheitlichen Umstieg auf eine Cloud-Netzwerkmanagementlösung. Lediglich 1 von 10 Unternehmen will weiterhin an On-Premises-Lösungen festhalten.

Einführung einer Cloud-Netzwerkmanagement-Lösung

Basis: 159 Unternehmen | Filter: Netzwerkmanagementlösungen ausschließlich oder Mix On-Premises



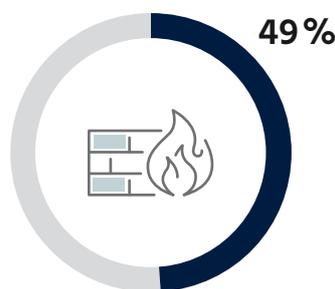
Die Gründe, die bei dem kleinen Anteil der Unternehmen vorherrschen, die sich gegen eine Cloud-Applikation entscheiden, sind überschaubar. Der Hauptgrund liegt in dem mangelnden Vertrauen in die Cloud-Technologie. Dies ist jedoch ein Sammelgrund, der sowohl Compliance-Bedenken als auch die Angst vor Zugriffsmöglichkeiten durch Dritte umfasst. Da das Netzwerkmanagement die kritische Infrastruktur jedes Unternehmens sicherstellt, müssen klare Zugriffs- und Rollenrechte vergeben werden. Niemand möchte, dass Geräte sich ins Netzwerk schleusen, um hochsensible Daten abzugreifen. Doch moderne und intelligente Netzwerkmanagementlösungen ermöglicht sowohl die Trennung von Zugriffsrechten je nach Netz als auch die Anwendungen innerhalb eines IP-Adressbereichs zu beschränken. Vordefinierte Rollen können dann auf das gesamte Netzwerk ausgeweitet werden.

Auch stellt die Cloud-Lösung Ansätze wie das Zero-Touch-Prinzip bereit, mit dem Geräte automatisch bereitgestellt und konfiguriert werden können. Der Prozess verläuft automatisiert und verhindert manuelle Eingriffe durch Fremdgeräte. Zusätzlich entfallen Tools, die vorher noch zur Konfiguration, Verwaltung oder dem Monitoring von Geräten nötig waren, komplett.

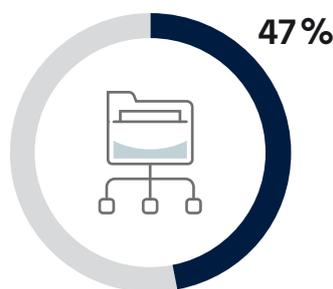
Jedes dritte Unternehmen (33 Prozent) sieht bereits die Vorteile durch Zero-Touch-Methoden.

Einsatzszenarien für gewonnene Informationen aus dem Netzwerkmanagement, um die Netzwerksicherheit zu erhöhen

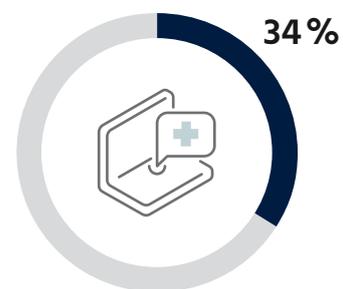
Basis: 200 Unternehmen | Mehrfachnennungen



Cyberangriffe und sicherheitsrelevante Incidents verfolgen können



Asset-/Inventory Management etablieren



Gerätezustand/Healthcheck erfassen können

Wenn Unternehmen zusätzlich auf Anbieter mit EU-Hauptsitz oder gar „Made in Germany“ zurückgreifen, kann auch die Datensicherheit und Compliance garantiert werden: Bedenken aufgrund von DSGVO-Bestimmungen brauchen diese Unternehmen dann nicht mehr haben. In Summe sieht sogar jedes zweite der befragten Unternehmen (50 Prozent) den größten Vorteil der Cloud-Lösung in der damit geschaffenen Datensicherheit und -integrität. Denn die Lösungen kommen nur in Verbindung mit Security-Dashboards, Intrusion Detection/ -Prevention und Firewalls als Secure Web Gateways – also ein ganzheitliches Paket für Netzwerksicherheit.

Ein weiterer Vorteil der Cloud-Lösung ist die Entlastung der eigenen Mitarbeiter (vor allem IT-Mitarbeiter). Große Projekte mit vielen Geräten erforderten bisher eine individuelle Konfiguration aller Geräte. Diese Konfiguration wird normalerweise nur am Installationsort vorgenommen. Treten Probleme oder Störung auf, wird häufig mit dem Trial-and-Error-Prinzip gesucht. Dafür braucht es hoch qualifiziertes IT-Personal und viel Zeit. Bei dem Netzwerkmanagement aus der Cloud übernimmt der Anbieter sämtliche Wartung, Pflege und Instandhaltung des Netzwerkes. Durch Zero-Touch-Bereitstellung werden neue Netzwerkkomponenten einfach hinzugefügt, eingerichtet und angeschlossen. Durch die anschließende automatische Konfiguration über Software-Defined Networking (SDN) muss die IT-Abteilung das Gerät nicht einmal mehr

anfassen oder vor Ort sein. Dies bedeutet, dass auch weniger qualifiziertes Personal Geräte installieren oder einrichten kann. Es benötigt lediglich einen Internetzugang. Dies nimmt den Unternehmen schwierige und zeitintensive Aufgaben ab. In Summe sehen 38 Prozent der befragten Unternehmen die Möglichkeit der Entlastung in den Bereichen Wartung, Instandhaltung und Pflege als relevanten Vorteil der Cloud-Lösung. Dadurch dass Unternehmen Zeit sparen, sparen sie bekannterweise auch Geld. Denn es werden zusätzlich kostspielige, redundante und komplexe Monitoring- und Analyse-Tools durch Cloud-Dienste konsolidiert. Hierdurch erkennen 48 Prozent der Unternehmen eine Möglichkeit der Kostensenkung durch Cloud-Netzwerkmanagementlösungen. Zudem sehen weitere 34 Prozent der Unternehmen die transparenten und flexiblen Kostenmodelle der Netzwerkmanagement-Cloud-Lösungen als relevanten Aspekt innerhalb ihrer zukünftigen Netzwerkarchitekturplanung.

Außerdem können Geräteverwaltung durch Zero-Touch und Netzwerkgröße durch SDN schnell und individuell angepasst werden, was den Unternehmen Vorteile in den Bereichen Flexibilität und Skalierbarkeit bietet. Mehrere Standorte können schnell und unkompliziert verbunden werden. Mehr als jedes dritte Unternehmen (37 Prozent) sieht darin einen sehr relevanten Vorteil des Netzwerkmanagements aus der Cloud.

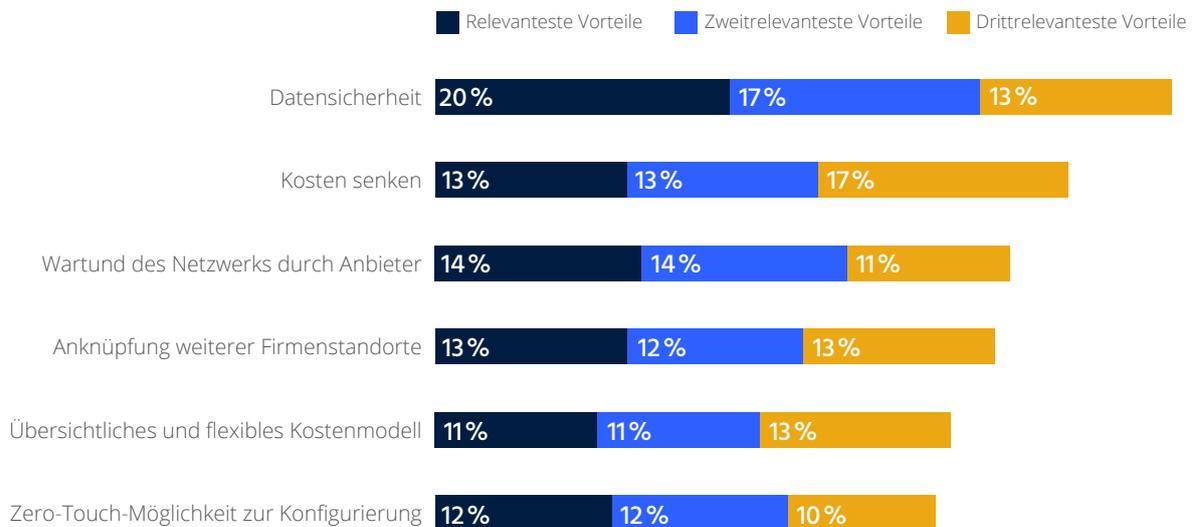
Weitere relevante Vorteile einer Cloud-Netzwerkmanagementlösung:

- Minimierung der Ausfallzeiten
- Erhöhte Transparenz im Netzwerk
- Möglichkeit für Predictive Maintenance (vorausschauende Wartung) von Netzwerkkomponenten
- Intelligente Benachrichtigungen (z. B. konfigurierbare Alarmer)
- Ermöglichung digitaler Geschäftsprozesse und den Zugriff auf die künstliche Intelligenz.



Benennung der relevantesten Vorteile einer Netzwerkmanagementlösungen aus der Cloud

Basis: 200 Unternehmen | Mehrfachnennungen



Fazit

Zusammenfassend lässt sich nun sagen, dass auch innerhalb des Netzwerkmanagements der Trend Richtung Cloud geht: 85 Prozent der Unternehmen wollen in den kommenden Jahren auf Cloud-Lösungen im Bereich des Netzwerkmanagements setzen. Sie erhoffen sich damit, neue und intelligente Technologien nutzen zu können, um mit dem digitalen Wachstum der Netzwerke mithalten zu können. Nicht verwunderlich stellen die befragten Unternehmen mangelhafte Netzwerktransparenz, häufig fehlende Automatisierung und fehlendes Fachwissen als Schwachstellen im Netzwerkmanagement fest. Außerdem erkennt mehr als jedes zweite Unternehmen Probleme und Bedenken im Bereich der Netzwerksicherheit. Kommen noch Herausforderungen wie lange Ausfallzeiten durch Fehlerbehebungen, aufwendiges Monitoring sowie Einrichten und Bereitstellen neuer Geräte hinzu, ist das Chaos für Netzwerkadministratoren vollständig. Ein Unternehmen ohne geregeltes Netzwerkmanagement kann dann den heutigen Standards kaum noch gerecht werden.

Doch den meisten der genannten Herausforderungen kann durch eine Migration des Netzwerkmanagements in die Cloud Abhilfe geschaffen werden. Ausfallzeiten und Latenzen werden minimiert, Flexibilität wird gefördert, die Netzwerksicherheit wird erhöht und die Administrationsaufgaben reduziert. Zero-Touch-Bereitstellung erleichtert das Hinzufügen, Einrichten und Verbinden neuer Netzwerkkomponenten.

Über Software-Defined Networking (SDN) muss die IT nicht einmal das Gerät anfassen oder im Unternehmen sein. Durch den Einsatz von integrierten Security-Dashboards, Angriffserkennung, Firewalls und Virendatenbanken wird ein stets aktueller Sicherheitsschirm durch den Provider garantiert. Aber auch flexible Zugriffs- und Userrechte erleichtern und schützen gleichzeitig die Netzwerkarbeiten durch Administratoren.

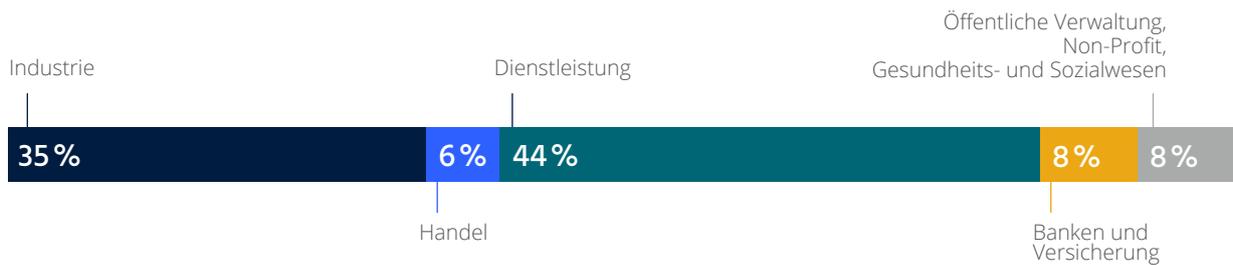
Andersrum können Unternehmen, die ihre Netzwerke als Selbstläufer betrachten, schnell ihre Geschäftsintegrität gegenüber Partnern und Kunden verlieren. Bereits kleinere Fehlkonfigurationen von eingesetzten Geräten an einem Standort können zum sicherheitsrelevanten Vorfall des gesamten Unternehmens werden. Und eins ist sicher, durch die Digitalisierung, Homeoffice und Gerätevernetzung werden in Zukunft nicht weniger Geräte im Netzwerk vorzufinden sein. Unternehmen benötigen damit ein dynamisches und effektives Managementwerkzeug, um Netzwerksicherheit und Integrität sicherzustellen. Das zeigt, dass Netzwerkmanagement, vor allem aus der Cloud, für eine effiziente Arbeitsweise in der Zukunft unabdingbar geworden ist.

Studiensteckbrief

Für die Studie „Moderne Standortvernetzung: Mit skalierbaren und sicheren Verbindungen für die Zukunft gerüstet!“ wurden 201 IT-Experten aus 5 Branchen über alle Unternehmensgrößenklassen in DACH/Benelux befragt. Als Qualifizierungsmerkmal wurden neben der Eignung als IT-Experte auch die Anzahl der Zweigstellen des Unternehmens herangezogen.

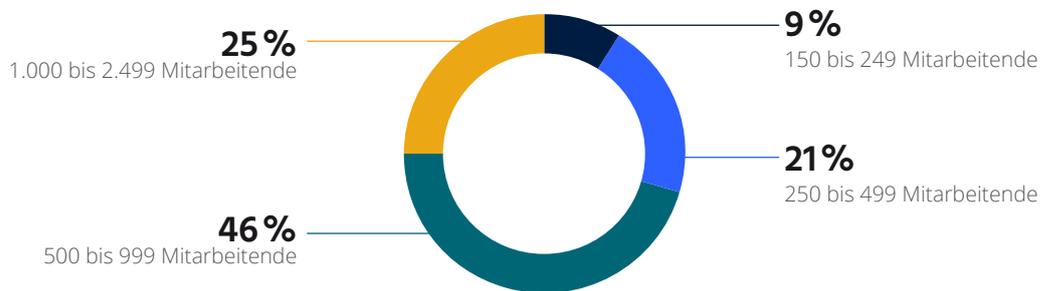
Befragte Branchen innerhalb der Studie

Basis: 200 Unternehmen



Befragte Unternehmensgrößenklassen der Studie

Basis: 200 Unternehmen



Anzahl der eingesetzten Netzwerkgeräte der Unternehmen dieser Studie

Basis: 200 Unternehmen



Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Erscheinungsdatum: 11/2022

Weitere Informationen

Impressum

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: info@techconsult.de

Tel.: +49 561 8109 0

Fax: +49 561 8109 101

Web: www.techconsult.de

Autoren

Waldemar Klassen
Analyst

Tel.: +49 561 8109 174

E-Mail: waldemar.klassen@techconsult.de

Giacomo Rogaia
Assistant Analyst

E-Mail: giacomo.rogaia@techconsult.de

Über die techconsult GmbH

Als Research und Analystenhaus ist techconsult seit 30 Jahren der Partner für Anbieter und Nachfrager digitaler Technologien und Services. Die techconsult GmbH wird vom geschäftsführenden Gesellschafter und Gründer Peter Burghardt am Standort Kassel mit einer Niederlassung in München geleitet.

ÜBER LANCOM Systems GmbH

Die LANCOM Systems GmbH ist führender europäischer Hersteller von Netzwerk- und Security-Lösungen für Wirtschaft und Verwaltung. Das Portfolio umfasst Hardware (WAN, LAN, WLAN, Firewalls), virtuelle Netzwerkkomponenten und Cloud-basierendes Software-defined Networking (SDN).

Soft- und Hardware-Entwicklung sowie Fertigung finden hauptsächlich in Deutschland statt, ebenso wie das Hosting des Netzwerk-Managements. Besonderes Augenmerk gilt der Vertrauenswürdigkeit und Sicherheit. Das Unternehmen hat sich der Backdoor-Freiheit seiner Produkte verpflichtet und ist Träger des vom Bundeswirtschaftsministerium initiierten Vertrauenszeichens „IT-Security Made in Germany“.

LANCOM wurde 2002 gegründet und hat seinen Hauptsitz in Würselen bei Aachen. Zu den Kunden zählen KMU, Behörden, Institutionen und Großkonzerne aus aller Welt. Seit Sommer 2018 ist das Unternehmen eigenständige Tochtergesellschaft des Münchner Technologiekonzerns Rohde & Schwarz

Kontakt

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Würselen
Deutschland

Telefon: +49 (0)2405 49936 0

Fax: +49 (0)2405 49936 99

E-Mail: info@lancom.de

Web: www.lancom-systems.de

LANCOM
SYSTEMS