DIN ISO/IEC 27001 ZERTIFIZIERT | DIN ISO/IEC 27001 ZERTIFIZIERT | CLOUD-DIENSTE 27018 GEPRÜFT | DIN EN ISO 9001 ZERTIFIZIERT | RECHENZENTRUM ECB•S ZERTIFIZIERT | KAMP GOES GREEN | DEUTSCHER RECHENZENTRUMSPREIS 2014 3. PLATZ KATEGORIE 10. GESAMTHEITLICHE ENERGIEEFFIZIENZ IM RZ

KAMP

24/7/365 Magazin

Die Kunden- und Informationszeitung der KAMP Netzwerkdienste GmbH /// Ausgabe Dezember 2017

Top-Thema: Next-Generation Firewalls im Focus

Was zeichnet Next-Generation Firewalls aus und warum bieten sie weitreichenden Schutz vor Angreifern?

Mehr auf Seite 2

Trend: IoT in Unternehmen

Internet of Things (IoT) ist mehr als Wirtschaftsmotor und Wettbewerbsfaktor. Wir beleuchten worauf es ankommt.

Mehr auf Seite 3

Moderne Vernetzungstechnologie im Einsatz

Die Diakonie Miachaelshoven setzt auf eine neue, zukunftsfähige Vernetzung von über 100 Standorten.

Mehr auf Seite 4

VORWORT

Herausforderung und Chance

In Zeiten voranschreitender Digitalisierung ist es heute für Unternehmen existenziell, sich den technischen Veränderungsprozessen zu stellen. Um aber bei der Menge an digitalen Neuerungen die Spreu vom Weizen zu trennen, hilft es einen IT-Partner an seiner Seite zu wissen, der Zukunftstechnologien aktiv mitgestaltet und sich gegen kurzlebige Trends absetzt. Getreu diesem Grundsatz agiert KAMP seit über 25 Jahren am Markt.

So freuen wir uns Ihnen heute ein neues, kostenfreies Leistungspaket unserer datenschutzkonformen Business-Cloud „KAMP DHP“ vorzustellen, das laut Heise „eine klare Kampfansage“ an amerikanische Anbieter wie Amazon oder Vultr darstellt. Lesen Sie in der aktuellen 24/7/365, warum ein MPLS-Netzwerk von KAMP für über 100 Standorte die richtige Option ist und weshalb Ciscos Next Generation Firewalls ein Plus an Sicherheit bieten.

Wir freuen uns für Sie aktiv zu sein.

Heiner Lante | Michael Lante

IMPRESSUM

Herausgeber: **KAMP Netzwerkdienste GmbH**
Vestische Straße 89–91
46117 Oberhausen

info@kamp.de
www.kamp.de

Redaktion: Danny Sternol
Barbara Blecker
Agnieszka Tielsch

Fotos KAMP, Shutterstock, Bilder Titelleiste 18871618 von ivra, 387267670 von wavebreakmedia, 383606608 von Wondervisuals

INFRASTRUCTURE AS A SERVICE

Das neue KAMP DHP Minipaket – der kostenfreie Einstieg in die Cloud

Schneller Informationsfluss, flexible Ressourcen und nahezu grenzenlose Skalierbarkeit gehören zu den unbestrittenen Vorteilen von Cloud-Lösungen für Unternehmen. Darum bietet KAMP mit dem Dynamic Hardware Pool (KAMP DHP) seinen Kunden eine datenschutzkonforme und sichere IaaS-Plattform an. Testen Sie jetzt, wie sich die Cloud in der Praxis präsentiert – kostenfrei und ohne Zeitdruck

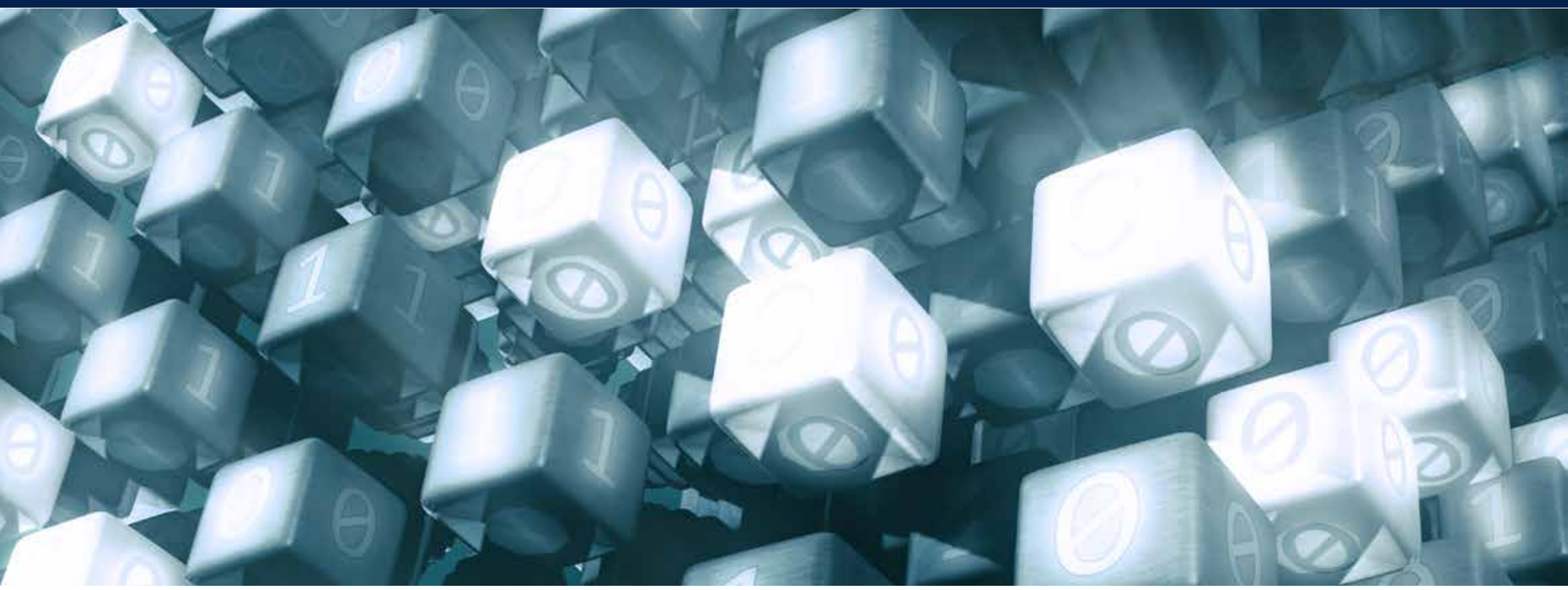
Software Hosted in Germany – Bundesverband IT-Mittelstand e.V.

Um Unternehmen den Einstieg in deutsche, und damit datenschutzkonforme, Cloud-Lösungen zu erleichtern, hat KAMP seine Infrastrukturplattform DHP (Dynamic Hardware Pool) jetzt um ein kostenfreies Leistungspaket erweitert. Unverbindlich und ohne zeitliche Einschränkungen können Interessierte sich von der Qualität der IaaS-Plattform überzeugen und sie unter realen Bedingungen testen. Der Leistungsumfang des sogenannten „Minipaketes“ umfasst 1 vCPU, 1 GB RAM, 25 GB Storage und 10 GB Traffic pro Tag und verfügt über eine 1 Gbit/s Anbindung zum Internet.

Das neue Minipaket enthält zudem viele Features, die KAMP DHP Kunden von den bislang vorhandenen kostenpflichtigen Paketen kennen: Dank des kompletten Root-Zugriffs kann der angelegte vServer uneingeschränkt und nach eigenen Bedürfnissen eingerichtet und installiert werden. Eine frei konfigurierbare Firewall und Zwei-Faktor-Authentifizierung sorgen für die nötige Anwendungssicherheit. Die meistgenutzten Linux-Distributionen Ubuntu, Debian und CentOS und über 100 schlüsselfertige Appliances sind bei dem in KAMP DHP kostenlos angelegten vServer ebenfalls inklusive. Die Lizenzkosten für Microsoft Windows Server 2012 R2 und 2016 sind ab dem kostenpflichtigen Starterpaket enthalten. ▪

KAMP DHP	RAM	Storage	DLP	Traffic/Tag	Preis/Tag
Minipaket	1 vCPU	1 GB	25 GB	10 GB	0,00 €
Starterpaket	6 vCPUs	8 GB	200 GB	25 GB	1,70 €

*Alle Preisangaben: Kalendertägliche Nettoentgelte in Euro, zuzüglich der gesetzlichen Mehrwertsteuer.



18871618 von ivra

TOP-THEMA

Netzwerksicherheit der nächsten Generation!

Next-Generation Firewalls bieten weitreichenden Schutz vor Angreifern aus dem Netz. Die Bedrohung sensibler Unternehmensdaten durch komplexe Malware wie Spionagesoftware oder Trojaner ist allgegenwärtig. Um die Risiken zu minimieren und Kunden einen bestmöglichen Schutz zu gewährleisten, bietet KAMP neben klassischen Firewall-Systemen auch den Einsatz moderner Cisco Next-Generation Firewalls (NGFW) mit FirePOWER Services an. 24/7/365 erklärt, wie die NGFWs funktionieren und welche Vorteile sie bieten.

Die Gefahren, die im Netz lauern, sind allgemein bekannt: Cyberkriminelle verschaffen sich Zugriff auf sensible Unternehmensdaten. Schadsoftware wird eingeschleust, Unternehmen werden ausspioniert und Daten verändert oder gelöscht. Wie verheerend die Schäden sein können, haben dieses Jahr Unternehmen weltweit zu spüren bekommen, als die Schreckensmeldungen der globalen Cyberattacke „WannaCry“ durch die Medien gingen. Mitte Mai breitete sich die Ransomware im Internet aus und befiel Rechner aus aller Welt. Der Kryptotrojaner verschlüsselte Computerdaten und gab den Schlüssel zum Dekodieren nur gegen ein Lösegeld wieder frei. Besonders schwere Folgen hatte der Hackerangriff in Großbritannien, wo der Trojaner zahlreiche Rechner in Krankenhäusern des National Health Service (NHS) befiel und dort chaotische Zustände auslöste. WannaCry machte aber auch vor Ministerien, Banken, Behörden oder Unternehmen nicht Halt. Nach Angaben der europäischen Polizeibehörde Europol waren weltweit mindestens 200.000 Computersysteme in 150 Ländern betroffen. Prognosen sehen die Häufung solcher oder ähnlicher Vorfälle voraus und machen sehr deutlich wie wichtig es ist, Firmen- und Datennetzwerke gegen Angriffe zu schützen. Ein wichtiger Bestandteil eines durchdachten Sicherheitskonzeptes ist dabei die Firewall, die in keinem Netzwerk mit Anbindung zum Internet fehlen darf. Die „Schutzmauer“ dient dabei als Filter: Auf Grundlage von definierten Sicherheitsregeln überwacht sie den eingehenden und ausgehenden Datenverkehr und entscheidet, ob bestimmte Verbindungen zugelassen oder blockiert werden.

Die Guten ins Töpfchen, die Schlechten ins Kröpfchen

Was im Märchen recht mühelos klingt, erweist sich in der Realität jedoch als Herausforderung. „Die Schlechten“ zu identifizieren wird in einer komplexen Bedrohungslandschaft für herkömmliche Firewalls, die auf Basis von Port- und IP-Adressen-Überprüfung arbeiten, zunehmend schwieriger. Zum einen arbeiten Hacker sehr schnell, um neue Varianten bösartiger Malware zu entwickeln und gehen gezielt vor, jede Lücke in der Abwehr auszunutzen. Zum anderen ist die Nutzung von sozialen Netzwerken wie Facebook oder Twitter, Instant Messengern oder das Verwenden von Programmen wie Skype oder Facetime unter Mitarbeitern längst weit verbreitet. Diese Dienste zeigen sich jedoch besonders anfällig gegenüber Viren oder Malware. Hinzu kommt, dass immer mehr mobile Endgeräte wie Smartphones oder Handys mit dem Unternehmensnetzwerk verbunden sind. Konkret muss eine moderne Firewall also Applikationen erkennen und zwischen ihnen unterscheiden können. Da hinter den Anwendungen aber auch Benutzer stehen, braucht es neben dieser „Application Awareness“ auch noch „Content- und User Awareness“. Dies setzt komplexes Konfigurations-Know-how und entsprechende Manpower voraus. KAMP ist sich dieser Herausforderung sehr bewusst und bietet deshalb seinen Kunden den Einsatz einer modernen Next-Generation Firewall, der Cisco ASA mit FirePOWER, auch als Managed-Service an. Durch das „Mieten“ einer Firewall bekommen Unternehmen ein rundum Sorglos-Paket, bei dem sich speziell geschultes Personal bei KAMP nicht nur um eine genaue Netzwerkanalyse kümmert, sondern auch um die saubere Planung und professionelle Umsetzung. Im Ergebnis erhalten Kunden eine perfekt auf ihre Bedürfnisse angepasste Firewall, inklusive aller Firm- und Softwareupdates.

Alles im Blick

Eine Next-Generation Firewall, kurz NGFW, kombiniert die Features herkömmlicher Firewalls wie Paketfilterung, Network Address Translation und VPN mit modernen Funktionalitäten wie Intrusion Prevention System (IPS), URL-Blockierung, Reputations-basierter Malware-Abwehr oder Applikationskontrolle. Die von KAMP angebotene Cisco ASA mit FirePOWER bietet eine integrierte Abwehrlösung mit mehr Funktionen für die Erkennung von Bedrohungen als andere Hersteller. Während klassische NGFWs ihre Aufmerksamkeit auf die Verfügbarkeit und Steuerung von Anwendungen richten, greift Cisco auf umfangreiche Cloud-Netzwerke mit Sicherheitsinformationen von Talos zurück und stellt sie der integrierten Analyse- und Schutzlösung der Cisco ASA Firewall zur Verfügung. Die Talos Security Intelligence and Research Group ist ein Team aus hochqualifizierten Sicherheitsexperten. Sie untersuchen die weltweite Bedrohungslandschaft auf Gefahren und analysieren zu diesem Zweck Telemetriedaten zu Milliarden von Webanfragen und E-Mails, Millionen von Malwareproben sowie Millionen von Network-Intrusion-Versuchen, um sie anschließend an das Cisco CSI-Netzwerk (Collective Security Intelligence) zu übermitteln. Identifiziert das System eine Bedrohung, wird innerhalb weniger Minuten an allen Standorten weltweit automatisch ihr Datenverkehr blockiert, verworfen oder in Quarantäne gestellt. Dabei gibt es in dem System von Cisco die Möglichkeit eines Botnet-Filters, der die Kommunikation von Botnet-Clients mit ihren C&C Servern erkennen und unterbinden kann. Die Erkennung basiert auf Blacklists mit verschiedenen Kategorien und Risikoklassen.

Um diese zunehmend komplexen Regeln und dynamischen Filtermerkmale zu verwalten, müssen die Managementoberflächen der NGFWs übersichtlich und bedienbar gehalten werden. Bei Cisco behalten Administratoren den Überblick über alle Vorgänge und verwalten sämtliche Prozesse im Management Center, dem Kontrollzentrum der Cisco ASA mit FirePOWER Services. Hier werden Benutzer, Hosts, Anwendungen, Bedrohungen und Schwachstellen in einer klar strukturierten Oberfläche dargestellt. Der Administrator erhält einen Überblick über sämtliche Aktivitäten im Netzwerk und kann Anwendungen sowohl überwachen als auch Malware-Outbreaks erkennen und untersuchen. „Die umfassenden Kontrollmöglichkeiten machen die Nutzung des Netzwerks sehr transparent“, so Tobias Schmidt, technischer Leiter bei KAMP.

„Auf dem Files Dashboard, der Hauptansicht, kann man beispielsweise nicht nur erkennen, welcher Nutzer welche Dateien heruntergeladen hat, sondern auch die gesamte Datei-Historie nachvollziehen – also wo eine Datei herkommt, an wen sie zwischenzeitlich weitergeleitet wurde und wohin sie letztlich verschickt wurde.“ In einer weiteren Ansicht, in der „URL & Web Filter“ angezeigt werden, können Zugriffsberechtigungen zu einzelnen Internetseiten und Applikationen verwaltet werden. Hier lassen sich sogar für jede Mikro-Applikation eigene Regeln erstellen: „Man könnte bestimmte Funktionen blockieren, wie beispielsweise den Like-Button bei Facebook“, erklärt Tobias Schmidt. „Und

es ist möglich, Berechtigungen einzelnen Benutzergruppen zuzuordnen, sodass Mitarbeiter in unterschiedlichen Tätigkeitsbereichen und Positionen auch verschiedene Zugriffsrechte erhalten.“ Natürlich lassen sich auch Webseiten mit unerwünschten Inhalten generell blockieren. Hierfür kann man aus einem Katalog mit über 3.000 Risikokategorien auswählen, welche Inhalte unerwünscht sind. So würde Nutzern der Zugang zu Themen wie beispielsweise Gewalt, Rassismus, Hass oder Waffen grundsätzlich verweigert.

Datenschutz und Compliance

Mit ihren umfangreichen Kontrollmöglichkeiten ist die Cisco ASA mit FirePOWER Services ein wirksames Tool, um Sicherheitslücken zu minimieren und Gefahren aus dem Netz die Stirn zu bieten. Jeglicher Überwachung des Netzwerkverkehrs stehen jedoch auch immer geltende Datenschutzgesetze und der Schutz der Privatsphäre entgegen. Um die Vorteile einer NGFW in Unternehmen gewinnbringend einsetzen zu können ist es daher sinnvoll, alle beteiligten Mitarbeiter über den Zweck und Nutzen, aber auch die Konsequenzen der Maßnahme, aufzuklären. Ein unternehmensinternes Compliance-Management kann hier für Transparenz sorgen. In vielen deutschen Unternehmen sind Compliance-Regelungen bereits zu einem wichtigen Bestandteil der Corporate Governance geworden. Häufig werden eigens für die Einhaltung der festgelegten Richtlinien Compliance-Beauftragte eingesetzt. In ihre Zuständigkeit fällt, in Zusammenarbeit mit Datenschutzbeauftragten, die Verantwortung, die eingesetzten Firewall-Regelungen und die damit verbundenen Überwachungs- und Restriktionsmöglichkeiten, offen darzulegen. Unmut und Misstrauen gegenüber dem System kann somit effektiv vorgebeugt werden.

Immer einen Schritt voraus

Cyber-Attacken auf die Datennetzwerke von Unternehmen werden in den nächsten Jahren stark zunehmen, da sind sich Experten einig. Dabei wird heute bekannte Malware kontinuierlich weiterentwickelt und modifiziert. Um das eigene Netzwerk auch zukünftig gegen Cyber-Kriminelle optimal zu schützen, müssen Abwehrmaßnahmen ebenfalls dynamisch auf die Gefahrenlage angepasst und stets auf dem neusten Stand gehalten werden. Sicherheit ist daher stets als Prozess zu verstehen. Next Generation Firewalls wie die Cisco ASA mit FirePOWER Services stellen hier, durch die aufeinander abgestimmte Sammlung von Abwehrfunktionen und Security-Lösungen, eine zeitgemäße Sicherheitskomponente dar. Weil eine NGFW jedoch immer erst unter Einsatz des entsprechenden Know-hows ihre volle Wirkung entfalten kann, bietet KAMP alles aus einer Hand: von der Konzeption durch geschulte Security-Experten bis hin zum kompletten Management der Firewall. Von zentraler Bedeutung für die Unternehmenssicherheit ist dabei eine an die IT-Umgebung angepasste Konfiguration, die dem Geschäftsmodell des Kunden entspricht und seine unternehmenseigenen Compliance-Regelungen berücksichtig. ▪

Shutterstock-ID 30574615

KAMP – WIR STELLEN UNS VOR

Auf eine gute Zusammenarbeit!

KAMP wächst weiter und begrüßt zwei neue Gesichter im Team. Wir freuen uns, Ihnen Frau Agnieszka Tielsch und Herrn Daniel Tönnißen vorzustellen.

Seit Februar unterstützt **Agnieszka Tielsch** die Marketing-Abteilung mit ihrem sprachlichen Geschick. Die studierte Anglistin kann mit ihren 39 Jahren auf reichlich PR-Erfahrung zurückblicken. Ihre Vorliebe, komplexe Themen verständlich zu transportieren, stellte sie in der Vergangenheit schon in der PR-Abteilung von RWE unter Beweis. Zusammen mit den Erfahrungen als freiberufliche Redakteurin im deutschen und englischsprachigen Umfeld, sowie als Texterin für Marketing-Medien, ist sie eine Bereicherung für die Öffentlichkeitsarbeit von KAMP.

Mit dem Vollblut-IT-ler **Daniel Tönnißen** erweitert zudem ein erfahrener Fachinformatiker unser Technik-Team. Der sportliche 35-Jährige verfügt über 13 Jahre berufliche Erfahrung. Nach einer fundierten Ausbildung zum Systemintegrator qualifizierte er sich konstant weiter, bis er verantwortlicher IT-Leiter eines börsennotierten Unternehmens wurde. Der lösungsorientierte Experte hat eine Vorliebe für neue Herausforderungen. Bei KAMP freut er sich zukünftig spannende, interdisziplinäre und technisch tiefgreifende IT-Projekte begleiten zu dürfen.

Agnieszka Tielsch oben; Daniel Tönnißen unten

IT-NEWS

Im Trend: Unternehmen setzen auf IoT

Industrie im digitalen Wandel: Mit vernetzten Geräten zu optimierten Produktionsabläufen und neuen Services.

IoT (Internet of Things), Digitalisierung und Industrie 4.0 gehören derzeit zu den meist diskutierten Themen in Handel und Wirtschaft. Denn die Zahl der Unternehmen, die auf digitalen Fortschritt setzen, steigt stetig: Laut einer Schätzung von Gartner werden bereits 2020 mehr als 20 Milliarden IoT-Geräte weltweit mit dem Internet verbunden sein. Vorreiter dieser Technologie finden sich heute vor allem bei größeren Firmen aus den Branchen Transport und Logistik, Dienstleistung und Gesundheit sowie dem produzierenden Gewerbe, wo die Möglichkeiten von IoT in unterschiedlichsten Szenarien genutzt werden. Die Vollautomatisierung innerbetrieblicher Abläufe und das kontinuierliche Auswerten von Daten ermöglichen dabei häufig, bestehende Produkte, Prozesse und Dienstleistungen zu optimieren und so die eigene Produktivität zu erhöhen. Eine stabile und sichere Vernetzung, eine leistungsfähige und hochverfügbare Infrastruktur sowie ein sicherer Speicherort für die entstehende Datenflut sind grundlegende Voraussetzungen, um IoT zu implementieren und die Möglichkeiten der Zukunftstechnologie vollumfänglich zu nutzen. KAMP stellt Unternehmen für die Umsetzung einer Vielzahl von IT-Projekten ein stabiles Fundament zur Verfügung. Mit einem sicheren und mehrfach zertifizierten Rechenzentrum als Basis, bietet KAMP vom eigenen Serverraum bis hin zur datenschutzkonformen und leistungsstarken Cloud-Plattform Unternehmen vielfältige Möglichkeiten, ihre IT-Vorhaben in einer hochverfügbaren Umgebung zu realisieren und zu betreiben. Um eine auf individuelle Begebenheiten optimierte Lösung zu erhalten, kombinieren Unternehmen dabei häufig Colocation mit Cloud-Computing oder eigenen, bereits vorhandenen, Server-Infrastrukturen. Mit modernster Vernetzungstechnologie, einem skalierbaren Leistungsangebot und entsprechendem technischen Know-how erweist sich KAMP als zuverlässiger Technologie-Partner für die erfolgreiche Realisierung von Digitalisierungsprozessen in Unternehmen. ▪

CASE STUDY

Vorausschauend vernetzt: Umfangreiche MPLS-Lösung für die Diakonie Michaelshoven

KAMP realisiert für den größten diakonischen Träger im Kölner Raum ein MPLS-Netzwerk mit einem zentralen Internet-Outbreak im zertifizierten KAMP-Rechenzentrum. Mit dieser MPLS-basierten Netzinfrastruktur verbindet KAMP über 100 Standorte der Diakonie Michaelshoven und das transparent, sicher und performant.

Mit Menschen Perspektiven schaffen

Seit über 60 Jahren unterstützt die Diakonie Michaelshoven Menschen in allen sozialen Belangen. Ursprünglich als Kinderheim gegründet, besteht die Diakonie heute aus über 100 unterschiedlichen Einrichtungen, in denen rund 2.000 Mitarbeiter und über 400 ehrenamtliche Helfer arbeiten. Unter dem Leitspruch: „Mit Menschen Perspektiven schaffen“, begleiten und fördern sie Menschen in unterschiedlichen Lebenslagen. Ein Großteil der Diakonie-Standorte befindet sich im Kölner Stadtteil Rodenkirchen. Die Außenstellen erstrecken sich dabei vom Rhein-Erft-Kreis über den Rhein-Sieg-Kreis und den Rheinisch-Bergischen Kreis bis hin zum Oberbergischen Kreis.

Ressourcen sparen mit modernen Netzarchitekturen

Die Größe des Unternehmens und die Tatsache, dass alle Standorte verschiedene Aufgabenbereiche haben, machen eine optimale Vernetzung unbedingt notwendig. Die einstige VPN-Netzstruktur verbrauchte jedoch zu viele Ressourcen und ließ sich nicht mehr arbeits- und kosteneffizient betreiben. Aus diesem Grund hat sich die Diakonie entschieden, auf ein modernes Multiprotocol Label Switching (MPLS) Netzwerk umzusteigen, das von einem externen Dienstleister betreut wird. Nach einer längeren Evaluierungsphase fiel die Wahl auf KAMP. Dabei konnte KAMP nicht nur aufgrund eines preislich attraktiven Angebotes, sondern auch beim Service und den technischen Möglichkeiten punkten. „Wir haben uns für KAMP entschieden, da uns der Rechenzentrumsbetreiber das optimale Gesamtpaket für eine sichere Standortvernetzung präsentiert hat“, erzählt Peter Gatzweiler, IT-Leiter der Diakonie Michaelshoven. „So hat uns KAMP eine maßgeschneiderte und vor allem zukunftsfähige IT-Vernetzung konzipiert, die mit unserer Einrichtung auch in den kommenden Jahren problemlos mitwachsen kann.“

Ein sicheres und schnelles Netzwerk

Um zukünftig schnell auf sich verändernde Leitungsanforderungen wie beispielsweise gesteigerte Bandbreiten reagieren zu können, hat KAMP bei der MPLS-Architektur zu einem zentralen und performanten Internet-Outbreak geraten. Durch die Realisierung des Internet-Outbreaks im KAMP-Rechenzentrum wird der Single Point of Failure, also die eine Schwachstelle, die den reibungslosen Betrieb des ganzen MPLS-Systems zum Erliegen bringen könnte, minimiert. Eine dedizierte Firewall sichert das System zusätzlich ab. Zur Anbindung der über 100 Standorte setzt KAMP bei der Realisierung des MPLS-Netzwerks auf den Technologie-Partner Deutsche Telekom. KAMP übernimmt dabei die Betriebsverantwortung für die MPLS-Anbindung und das Routing. Der komplette Betrieb der Anbindung wird von KAMP 24 Stunden, 7 Tage die Woche, 365 Tage im Jahr überwacht und verwaltet.

Maximale Sicherheit für zentrale MPLS-Strukturen

Für eine sozial-karitative Einrichtung mit sensiblem Datenbestand ist der Datenschutz enorm wichtig. Deshalb wurde im Voraus genau besprochen, was in Bezug auf die Sicherheit alles möglich ist. Das MPLS-Netzwerk ist vollständig vom Internet getrennt und somit vor unberechtigten Zugriffen von außen geschützt. Die Einwahl einzelner Standorte in die Unternehmens-MPLS der Diakonie erfolgt direkt im KAMP-Backbone. Im KAMP-Rechenzentrum, das nach der internationalen Norm ISO/IEC 27001 zertifiziert

436942042 von Sahacha Nilkumhang

Diakonie Michaelshoven – Vernetzung für über 100 Standorte

ist, sorgen neben den technischen Maßnahmen auch biometrische Zutrittskontrollen, Brandschutzanlagen und Frühwarnsysteme für den professionellen Schutz der Hardware, IT-Systeme und Daten. Dank der intelligenten Vernetzungsstrategie kann sich die IT-Abteilung der Diakonie nun wieder auf ihre Kernkompetenzen, die Arbeit mit den Menschen, konzentrieren. „Die maßgeschneiderte MPLS-Lösung von KAMP stellt für die Diakonie Michaelshoven eine sichere, zukunftsfähige und leistungsstarke Vernetzung der verschiedenen Standorte dar“, so Diakonie-IT-Leiter Peter Gatzweiler. „Wir freuen uns auf eine weiterhin reibungslose Zusammenarbeit.“ ▪

Lesen Sie die gesamte Case Study unter: www.kamp.de

WLAN-SERVICES

WLAN: Mit gründlicher Planung zu lückenlosem Empfang

Eine unzuverlässige WLAN-Verbindung ist im Privatleben meist ein Ärgernis. In digitalisierten Unternehmen dagegen oder in medizinischen Einrichtungen können Ausfälle folgenschwere Konsequenzen nach sich ziehen.

Ein kabelloses Netzwerk ist eine Technologie, mit der heute in vielen Branchen Arbeitsprozesse optimiert werden. So ist es beispielsweise im Bereich der medizinischen Versorgung von grundlegender Bedeutung, dass Patientendaten schnell und zuverlässig zur Verfügung stehen. Dank moderner WLAN-Technologie werden heute in vielen medizinischen Einrichtungen elektronische Patientenakten genutzt, Vitaldaten auch unterwegs kontrolliert und moderne Diagnosegeräte pflegen ihre Daten direkt ins Kliniknetzwerk ein. Dadurch gewinnt das Krankenhauspersonal wertvolle Zeit. Nicht zuletzt bietet WLAN auch Patienten mehr Komfort während eines Krankenhausaufenthaltes.

Gerade in medizinischen Einrichtungen sind Funklöcher oder Signalschwankungen jedoch absolut inakzeptabel. Um Fehlinvestitionen zu vermeiden und mögliche Störquellen im Vorfeld zu identifizieren, sind professionelle Beratung und vorausschauende Planung sowie eine gründliche Untersuchung der örtlichen Gegebenheiten wichtige Voraussetzungen. Dank langjähriger Erfahrungen im Aufbau von WLAN-Netzwerken, weiß KAMP um die Anforderungen an eine ideale Netzwerk-Architektur und bietet bedarfsorientierte Lösungen nach allen verfügbaren WLAN Standards an. Von zentraler Bedeutung ist dabei eine exakte Ausleuchtung, also eine genaue technische Erfassung der baulichen Situation durch Messungen vor Ort. Sie bildet die Grundlage für den KAMP-Vermessungsbericht. Dieser Bericht visualisiert anschaulich die optimale Platzierung und Anzahl der Access Points, Signalstärken, Signalrauschen, Störquellen und eventuell störende Fremdnetzwerke. Eine flächendeckende und leistungsstarke WLAN-Versorgung wird bei KAMP in fünf Schritten realisiert:

1. Planungsphase

In dieser Phase werden die Anforderungen an das Netzwerk geklärt. Welche Bereiche sollen ausgeleuchtet werden, welche Hardware muss angebunden werden und welche Anwendungen sollen zum Einsatz kommen?

2. Simulationsphase

Mithilfe aufbereiteter, digitalisierter Bau- und Geländepläne wird der vom WLAN abgedeckte Bereich mit einer speziellen Software von unseren Spezialisten simuliert.

3. Ausleuchtungsphase

Mit einer speziellen Vermessungssoftware und speziellen Mess-Access-Points wird die Leistung des Netzwerks nach der Substitutionsmethode an den vorher simulierten Messpunkten vor Ort eingemessen und bestimmt. Anhand eines Trackingtools werden die Standorte der Access Points im Gebäude und die gemessene Signalstärke detailliert dokumentiert. Diese ermittelten Daten bilden die Grundlage für den KAMP-Vermessungsbericht und eine verbindliche Kostenabschätzung Ihres WLAN-Projekts.

4. Installationsphase

Der KAMP-Vermessungsbericht ermöglicht dann die exakte Verkabelung und Installation der Access-Points. Dies wird durch hauseigene Techniker erfolgen.

5. Konfigurations- und Prüfphase

Nach der Installation werden die Access Points vor Ort konfiguriert. Danach ist das WLAN zum Einsatz bereit. Auf Wunsch wird durch eine erneute Ausleuchtung des fest installierten WLANs die nun optimale Funktion dokumentiert. ▪