Firmennetze der Zukunft

SD-WAN auf dem Prüfstand



ERLEBEN, WAS VERBINDET.

Anforderungen an Unternehmensnetze

Unternehmensnetze haben einen klaren Auftrag: Anwender*innen bzw. Maschinen mit ihren Anwendungen so zu verbinden, dass die Anwendungsperformance stimmt. Es darf keine Ausfälle geben – und wenn doch, müssen diese schnell behoben werden. Angriffe aufs Netz gilt es abzuwehren, damit keine Daten unbefugt das Netz verlassen. Und: die Umsetzung von neuen Anforderungen darf das Geschäft nicht ausbremsen. Gleichzeitig steigt die Dynamik, mit der sich Anwendungen, Clouds und Standorte verändern.

Beispiel Cloud:
Haben Unternehmen vor einigen Jahren nur wenige Anwendungen in eine Cloud verschoben, sind Software as a Service und Multi-Cloud mittlerweile die Norm.

Beispiel IoT:
Geschäftsprozesse hängen davon ab, dass immer mehr verteilte Sensoren und Systeme zuverlässig Daten an die Clouds liefern und neue Befehle empfangen.



Warum diese Anforderungen immer schwerer erreichbar werden

Die Schwächen klassischer Netzarchitekturen mit zentralem Internet Breakout als Weg zu den Clouds werden von Monat zu Monat deutlicher:

- Am zentralen Internet Gateway kommt es zu Verstopfungen.
- Performance-Probleme treten bei weit von den Gateways entfernten Standorten auf, weil der Weg über das Zentrale Gateway zur Cloud einfach zu lang wird.
- Störungen am Gateway legen gleich die ganze Firma lahm, da eine alternative Route fehlt.
- Das Hacker- und Datenleck-Risiko steigt, da neue Sicherheitskonzepte, die den Zugriff auf Anwendungen regeln, schwer umgesetzt werden können.



Für die Eliminierung der Schwächen ist eine umfassende Transformation der Netzarchitektur nötig. Diese ist jedoch an Rahmenbedingungen gebunden:

- Das Netzbudget bleibt maximal gleich, um den Inflationsdruck in anderen Bereichen des Einkaufs zu kompensieren.
- Netze, Firewalls, etc. haben noch laufende Verträge bzw. Abschreibungen, die einen sofortigen Tausch wirtschaftlich unsinnig machen.
- Die IT-Teams sind mit bestehenden Initiativen derart ausgelastet, dass die Netzstrategie und deren Umsetzung nur langsam vorankommt.

Zudem kommen neue Anforderungen an Netzprovider:

- Klimaschutz und Nachhaltigkeit werden immer relevanter – und hängen auch von der Nachhaltigkeitsumsetzung der Netzpartner ab.
- Lieferprobleme und -verzögerungen nehmen zu.
- Die bisher langfristige Standortwahl erfährt eine neue Dynamik, etwa auf Grund von Brexit, Produktions-verlagerungen, War for Talents oder Covid.
- Datenschutz ist keine Selbstverständlichkeit. Die komplexe Welt der gesetzlichen Regulatorien muss von den Netzprovidern beherrscht werden.

Die Zukunft: Software Defined Networking

Abhilfe aus dem Dilemma versprechen softwaredefinierte Netzwerke, insbesondere Weitverkehrsnetze, im Englischen Wide Area Networks genannt (SD-WAN). Dabei gelten die Grundsätze:

Mobile First
Anwender*innen arbeiten überall, weltweit – mal am Standort, mal daheim.

Quality Internet
Das Internet ist DAS Netz – die Qualität der Transportnetze setzt den Rahmen für die gesamte Netz-Performance.

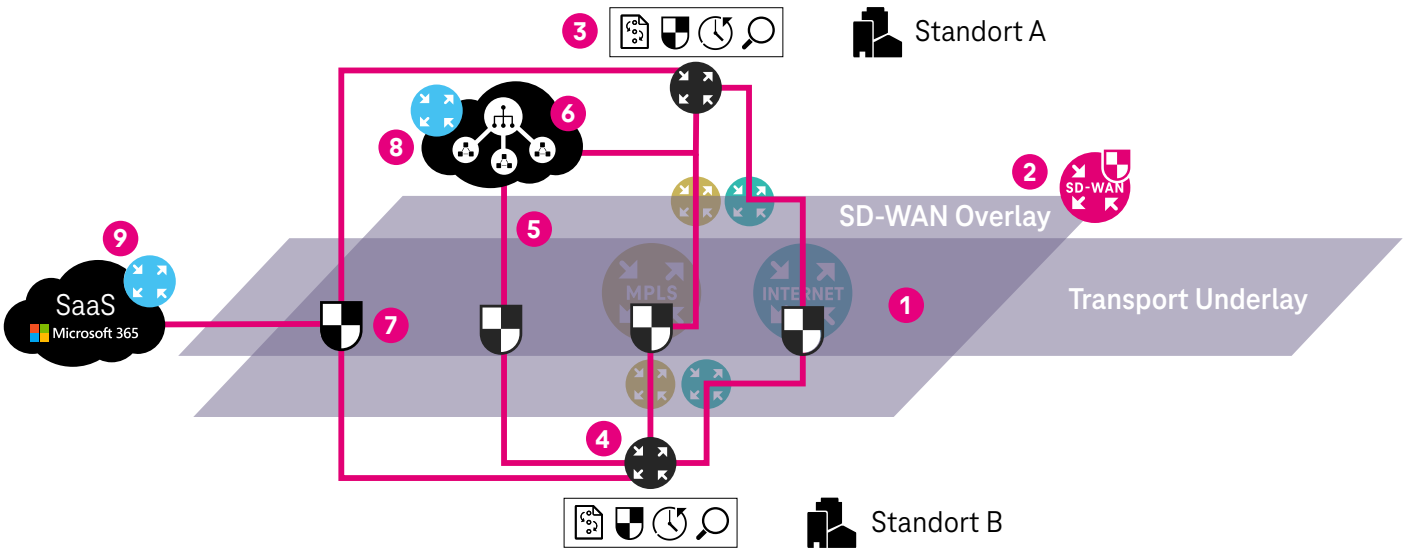
Automation
Ähnlich wie die Clouds sollen Netzdienste einfach und integriert für die IT-Mannschaft steuerbar sein.

Cloud First
Die Netze müssen sich mit den verschiedensten Clouds verbinden.

Global Support
Beispiel Brexit: die Politik verändert die Dynamik von Standorten und Lieferketten, die im Netz nachgezogen werden müssen.

Security First
Das Netz der Zukunft kann einfach State of the Art Security-Konzepte und -Komponenten integrieren und steuern.

SD-WAN-Architektur



1. Es werden für den Datentransport mindestens zwei Transportnetze genutzt, z. B. Internet, MPLS und mobiler Access. Diese Netze wurden auch bisher für Unternehmensvernetzung genutzt, z. B. für IP-VPN oder MPLS-Netze.

2. Die bisher genutzte Intelligenz wandert ins SD-WAN, dem so genannten Overlay.

3. Für das Overlay wird an den Standorten neue Software nötig (SD-WAN), die auf neuer Hardware läuft.

4. Die SD-WAN-Software spannt nun Tunnel zwischen den Standorten und zu Clouds auf.

5. Die Standorte und alle Funktionen werden über zentrale SD-WAN-Controller und Orchestrierungs-Software gesteuert. Hier liegen auch die Informationen über die Performance der Verkehrswege, die für die intelligente Steuerung verwendet werden.

6. Die zentralen Komponenten werden in Clouds betrieben.

7. Die Verbindung zu den Clouds über das Internet muss abgesichert werden. Dies geschieht durch Security Software, die (a) auf dem SD-WAN-Router, (b) als separate Hardware oder (c) als Web Security Service betrieben wird.

8. In den Clouds können virtuelle Router installiert werden, um die Cloud als vollwertiges Rechenzentrum ins Netz einzubinden.

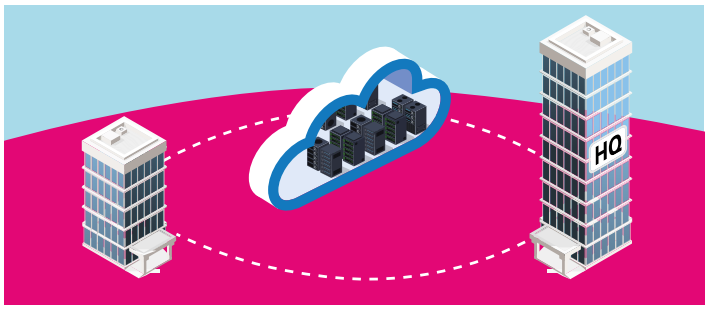
9. Die SD-WAN-Software steuert ebenfalls optimiert den Weg zu verschiedensten Software as a Service Angeboten wie z. B. Microsoft 365.

Mythos SD-WAN. Was ist dran?

Als die ersten SD-WAN-Angebote in den 10er Jahren dieses Jahrtausends auf den Markt kamen, entwickelten deren Hersteller zügig eine Vielzahl von Heilsversprechen. Im Folgenden prüfen wir sechs dieser Versprechen – lassen sie sich halten, und wenn ja, unter welchen Voraussetzungen?

Mythos 1

Je kürzer der Weg zur Cloud, desto besser



Stimmt das?

Nicht immer.

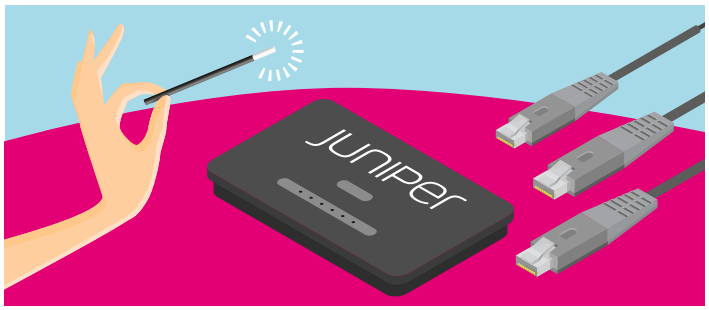
Ein übergreifendes Merkmal der SD-WAN-Architektur ist der lokale Internet Breakout. Statt über die Zentrale werden Clouds via lokalem Internet Breakout – abgesichert durch Security – stets auf direktem Weg erreicht, was auch weniger Latenz bedeutet.

Aber: Die Latenz hat keinen linearen Einfluss auf die Nutzererfahrung von Anwendungen, vielmehr macht sie sich für die meisten Anwendungen sprunghaft bemerkbar. So kann z. B. Netflix bis gut 1.300 km in 4K Streaming genossen werden – das Verkürzen auf z. B. 300 km macht den Stream nicht besser. Viele Apps bieten auch bei 2.000 km Entfernung zur Cloud und mehr gute Erlebnisse.

Zudem ist der direkte Weg über das Internet nicht immer der kürzeste. Die Wegstrecke hängt vor allem vom sogenannten Peering ab, also wie gut der Internet- (oder MPLS-) Provider mit den Clouds verbunden ist. Schlechtes Peering verlängert die Strecken.

Mythos 2

Zero Touch – Zero worries worldwide



Stimmt das?

Nicht ganz.

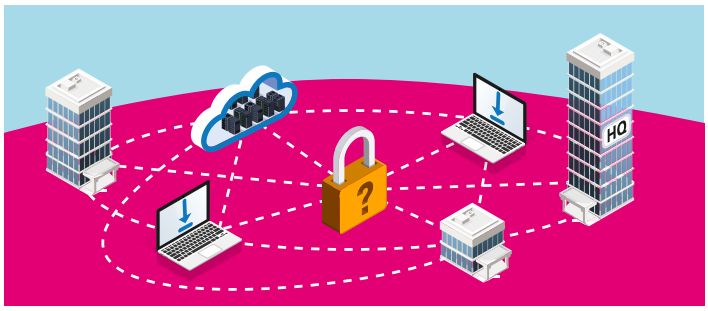
Eine weitere Eigenschaft von SD-WAN ist das „Zero Touch Provisioning“. Dahinter verbirgt sich die Vorstellung, dass nach der Verkabelung des Routers mit Strom, LAN und Transportnetzen alles Weitere selbstständig und ohne Expertenwissen vor Ort läuft. Manche SD-WAN-Anbieter suggerieren, Standort-Inbetriebnahmen gelängen nun im Handumdrehen: Via Same Day Delivery kommt die Hardware überall hin, die simple Skizze für die Verkabelung kann von jedem Mitarbeitenden verstanden werden – fertig.

Zero Touch ist in der Tat ein hervorragendes Werkzeug zur Vermeidung von Fehlerquellen bei der SD-WAN-Installation. SD-WAN-Router stehen jedoch meist nicht für sich, sondern werden in Server Racks mit weiteren IT-Geräten verbaut. Nicht jedes Unternehmen hat Mitarbeitende vor Ort, die diesen Einbau kompetent übernehmen können – so dass Field Services weiter eine Rolle spielen.

Und: Zero Touch ist der letzte Schritt einer langen Kette von Schrittfolgen in der Bestellung und Bereitstellung. Denn je nachdem, wo die auszustattenden Standorte sich befinden, müssen Provider die jeweiligen Konformitätsgesetze – z. B. Telekommunikationsgesetze – Steuern, Zölle und vieles mehr einhalten. Außerhalb der EU kann dieser Prozess sehr kompliziert werden. Global agierende Provider, die die benötigten Router-Typen idealerweise im jeweiligen Land selbst auf Lager haben, können hier die besten Konditionen anbieten. Auch gilt zu beachten: je exotischer ein SD-WAN-Router ist, desto schwieriger wird seine weltweite Bereitstellung.

Mythos 3

Mit SD-WAN ist alles sicher



Stimmt das?

Jein.

Die Netze der Zukunft benötigen eine neue Sicherheitsarchitektur. Konzepte wie „Zero Trust“, „Micro-Segmentation“ und „SASE“ schwirren umher. Wie relevant sind diese Konzepte?

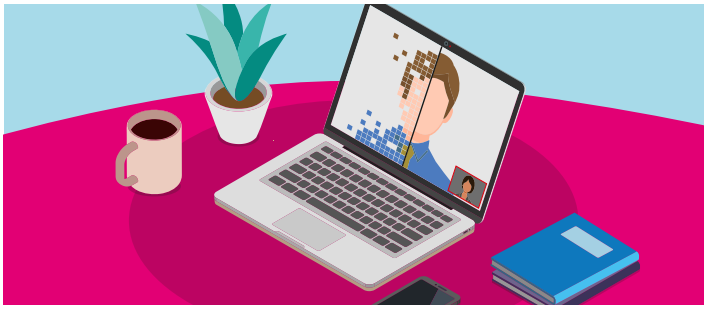
Eine kritische Komponente ist die Absicherung des Internetverkehrs gegen Ein- und Ausbrüche. In klassischen Netzen war der zu kontrollierende Punkt klar. Mit den dezentralen Internetzugängen an den Standorten und den mobilen Mitarbeitenden erhöht sich die Zahl zu kontrollierender Übergangspunkte enorm. Und je nach Anwender*in und Anwendung sind andere Sicherheitswerkzeuge von Nöten.

Abhilfe verspricht eine Architektur, für die das Beratungsunternehmen Gartner den Begriff SASE geprägt hat - Secure Access Service Edge. Die notwendigen Security-Komponenten werden dabei in vielen dezentral verteilten Clouds bereitgestellt, mit denen Anwender*innen sich via IP Sec Tunnel verbinden. Diese Standorte stellen die nötigen Security-Leistungen als Shared Service günstig und hochskalierbar bereit.

Aber ist SD-WAN ohne SASE unsicher? Unternehmen haben heute zahlreiche Security Services im Einsatz. Ein Umstieg ist wirtschaftlich meist erst mit Ablauf der Verträge oder Abschreibungen sinnvoll. Viele SD-WAN-Lösungen beinhalten zudem bereits Security Features. Es lohnt sich, deren Eignung auf die eigenen Belange zu prüfen. Eine weitere Möglichkeit: Neben dem Internetweg bieten private MPLS-Netze auch private Gateways zu den Hyperscalern. Security ist hier quasi eingebaut. Als Standard haben zudem fast alle SD-WAN-Services hochautomatisierte Zugänge zu den bekannten Web-Security-Anbietern. Deren Lizenzmodelle sind jedoch komplex. Zu bedenken gilt auch, dass eine Netz- und Sicherheitsarchitektur von verschiedenen Herstellern neben hohem Sicherheitsniveau auch hohe Komplexität für das Management mit sich bringt. Fazit: SASE ist eine Orientierung auf dem Weg zu einer neuen Sicherheitsarchitektur.

Mythos 4

SD-WAN liefert auch auf schlechten Netzen hervorragende Qualität



Stimmt das?

Nein.

Das Nutzererlebnis von Apps wird beim Datentransport neben der Latenz von weiteren Faktoren beeinflusst, zuallererst von Schwankungen in der Leistung, von der Verlustrate von Datenpaketen, dem Taktzittern (Jitter) in der Übertragung und der Häufigkeit von Störungen aller Art.

SD-WAN kann die Qualität der Übertragung positiv beeinflussen: Intelligentes Routing misst die Qualität der Übertragungswege, vergleicht diese mit den Anforderungen von Applikationen und lenkt deren Wege entsprechend der momentanen Qualität der Transportnetze. Für bestimmte Anwendungen nutzen SD-WAN-Technologien zudem Optimierungs-Algorithmen, am einfachsten gestaltet sich dies für Voice- und Video-Übertragungen.

Aber diese Kompensation benötigt ein paar Voraussetzungen: Die Gesamtleitungskapazität muss weit über der Nutzlast liegen, damit die alternativen Leitungen bei Ausfall eines Wegs nicht gleich verstopfen. Außerdem braucht die Verschlüsselung von SD-WAN Bandbreite, was einzukalkulieren ist. Und es muss mindestens ein hochqualitativer Weg vorhanden sein, der die wichtigen Anwendungen transportieren kann.

Temporäre Störungen in einem Netz, z. B. bei Ausfall, können alle SD-WAN-Anbieter durch intelligentes Routing und bei Vorhandensein von alternativen Netzen kompensieren.
Bei dauerhaften Qualitätsproblemen kann SD-WAN allein jedoch auch nicht helfen.

Mythos 5

Mehr Geld im Haus durch SD-WAN



Stimmt das?

Es kommt drauf an.

Ein von SD-WAN-Anbietern angeführter Vorteil ist die Aussicht, dass die Investitionen in SD-WAN sich durch massive Einsparungen in den Transportnetzen quasi von selbst finanzieren. Mit der Einführung von SD-WAN entstehen allerdings zunächst einmal Zusatzkosten für:

- Das SD-WAN selbst, mit Router-Hardware für Standorte und Softwarelizenzen
- Switching-Hardware an Standorten mit Hochverfügbarkeit
- Internet Security, z. B. Web-basiert oder auch vor Ort, falls die Security Features der gewählten SD-WAN-Lösung nicht ausreichen

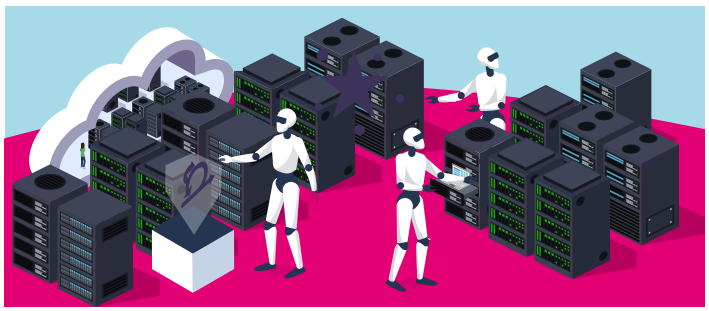
Bei den Einsparungen gehen die Anbieter davon aus, dass das bisherige Netz des Kunden auf MPLS beruht und der MPLS-Preis je MBit sehr viel teurer ist, als Internetzugang und Backbone, und dass SD-WAN etwaige Nachteile kompensiert.

Richtig ist auf jeden Fall, dass sich mit SD-WAN das Verhältnis MBit / Euro verbessern lässt: An den Standorten werden ergänzend oder alternativ Business Internet Anschlüsse sowie ggf. Consumer Grade Anschlüsse gelegt. Die MPLS-Bandbreite wird dann zu Gunsten des Premium Internet gesenkt und ggf. angereichert um Consumer Internet. Diese Maßnahme ist umso wirkungsvoller, je größer der Preisabstand zwischen MPLS und Business Internet ist, je größer der Bandbreitenbedarf ist, und je mehr Standorte dies betrifft.

Das gilt jedoch nicht für jeden Standort: Einsparungen lassen sich sehr gut an Standorten in den USA erzielen, wo der Preisabstand MPLS zu Business Internet sehr hoch ist – in Europa ist der Hebel geringer.

Mythos 6

Alles agil und automatisiert dank SD-WAN



Stimmt das?

Jein.

SD-WAN verspricht, die Vorlaufzeiten für Netzanpassungen und -konfigurationen drastisch zu senken und zu vereinfachen. Suggeriert wird weiterhin, dass durch automatisierte „Selbstheilung“ des Netzes die IT-Teams entlastet werden.

In der Tat verbessert sich für die IT-Teams mit SD-WAN so einiges: Das intelligente Routing verdeckt temporäre Störungen. Wo Anwender*innen früher direkt Störungsmeldungen aufgaben, kommen diese Störungen nicht mehr bei ihnen an. IT-Teams haben in der Folge weniger Tickets. Dank der Analyse-Dashboards, die mögliche Störungsquellen feingranular aufzeigen, reduzieren sich Zeit und Aufwand der Störungssuche zudem drastisch. Weiterer Pluspunkt: Konfigurationsänderungen, z. B. für Routingregeln, können schnell entworfen und für das ganze Netz ausgerollt werden.

Aber: SD-WAN ist nicht der einzige Baustein für die Automatisierung von Service-Management-Prozessen im Netz. Die Konfiguration eines SD-WAN-Netzes ist nicht „idiotensicher“, sie setzt Kompetenz für SD-WAN und Wechselwirkungen mit Transportnetzen und Security voraus. Dieses Knowhow müssen Unternehmen, ähnlich wie Cloud-Knowhow, sukzessive aufbauen. Die meisten Unternehmen kaufen Netze – auch SD-WAN – als managed Service ein. Sie sind somit darauf angewiesen, dass ihr Service-Partner Zugriff auf diese Funktionen erlaubt und dass dieser Zugriff auch datenschutz- und sicherheitskonform erfolgt.

Viele Geschäftsvorfälle im Netz benötigen zudem weitere Systeme, z. B. Billing-Systeme bei Lizenz-Upgrades oder Ticketing-Systeme zur Inzidenz-Steuerung. Fehlende Automatisierung lässt manche im SD-WAN gestarteten Prozesse wieder entschleunigen.

Zusammenfassung

Die Zukunft der Netze ist software defined: Niemals zuvor konnten so viele neue Netz- und Security-Services in so kurzer Zeit bereitgestellt werden. Cloud Connectivity, die Absicherung des Internetverkehrs oder tiefe Netzanalysen sind in der Komplexität nur per Software beherrschbar. Dabei besteht eine gegenseitige Abhängigkeit von Netz- und Security-Services, insbesondere was den effizienten Betrieb angeht.

SD-WAN ist kein Allheilmittel. Qualitätsprobleme mit Transportnetzen und deren Designs – ob Internet oder MPLS – können sehr gut sichtbar gemacht werden. Kompensieren kann SD-WAN sie jedoch höchstens temporär.

Eine Architektur für das Netz der Zukunft entsteht aus dem Zusammenspiel von SD-WAN-Transportnetzen, Security und den dafür nötigen Prozessen im IT-Service-Management. Mit der Reife von SD-WAN werden die Leistungsunterschiede zwischen den Technologien immer geringer. Der Fokus der IT-Verantwortlichen schiebt sich zunehmend auf die übergreifende Beherrschbarkeit und das Management über alle ITIL-Prozesse hinweg.



Die Deutsche Telekom bietet nicht nur ein Portfolio von leistungsfähigen SD-WAN-Lösungen, sondern mit der SD-X Plattform eine Management-Plattform, die auch weitere Services integrierbar und beherrschbar werden lässt.

SD-X: Grundstein für das Netz der Zukunft

Für das Management eines Netzes der Zukunft ist SD-WAN nur die Spitze des Eisbergs. Für einen wirklichen Produktivitäts- und Automatisierungssprung muss auch ein SD-WAN mit einer Vielzahl weiterer Systeme interagieren, z. B. für Bestellungen, Entstörungen oder dem LAN auf dem Campus. Ohne die Zusammenarbeit mit diesen Systemen werden viele Geschäftsvorfälle durch manuelle Schnittstellen ausgebremst.

Bisher stehen Unternehmen vor dem Problem, dass die meisten Service-Provider sich rein auf den technischen Betrieb des SD-WAN fokussieren. Eine Integration in ein IT-Service-Management bieten sie nicht an. Der Aufbau entsprechender Schnittstellen in Eigenregie ist für Unternehmen jedoch wirtschaftlich unverhältnismäßig teuer und komplex.

Es wird einfach:
Mit SD-X, der Software Defined Everything Plattform der Telekom, ändert sich das Spiel. Die SD-X Plattform automatisiert das Management der technischen UND alle weiteren Prozesse: IT-Service-Management und kommerzielle Prozesse von der Bestellung über die Konfigurationsänderung bis zum Inzidenzmanagement, von Changes und Reportings bis zu Analysen.

Die Zukunft beginnt jetzt:
Der erste Service auf der SD-X Plattform ist im Herbst 2021 gestartet: SD-WAN von der Telekom auf Basis von Juniper. Sie erhalten auf der Plattform zu dem State of the Art SD-WAN-Service mit integrierter Security eine Vielzahl vordefinierter Geschäftsvorfälle, die das Alltagsgeschäft deutlich entlasten und Prozesse beschleunigen.

SD-X wird erweitert:
Sukzessive werden immer mehr Netzwerk-Services auf diese Weise verfügbar gemacht: Vom SD-WAN über SD-LAN und WIFI bis zu SASE Services und Transportnetzen. Der Grundstein für das Netz der Zukunft ist mit der SD-X Plattform gelegt. Es wird software defined: hoch komfortabel und stabil nutzbar durch Automatisierung aller notwendigen Prozesse. Das ist unsere Vision.

Über den Autor



Axel Wegat ist SD-WAN Evangelist, führt die Markteinführung der Telekom SD-WAN Services und prägt auf Konferenzen die Diskussion um die Netze der Zukunft. Axel wohnt in München und ist zugleich Chef der Home Office Kantine seiner 5-köpfigen Familie. Nach Spülschluss ist er ein begeisterter Stand-Up Paddler und Radfahrer.

Noch Fragen?

Wir beraten Sie gerne ausführlich zum Thema SD-WAN.
Kontaktieren Sie uns.

sd-wan@telekom.de

Oder besuchen Sie unsere Website

Herausgeber
Telekom Deutschland GmbH
53262 Bonn
www.telekom.de

ERLEBEN, WAS VERBINDET.