CLOUDFLARE

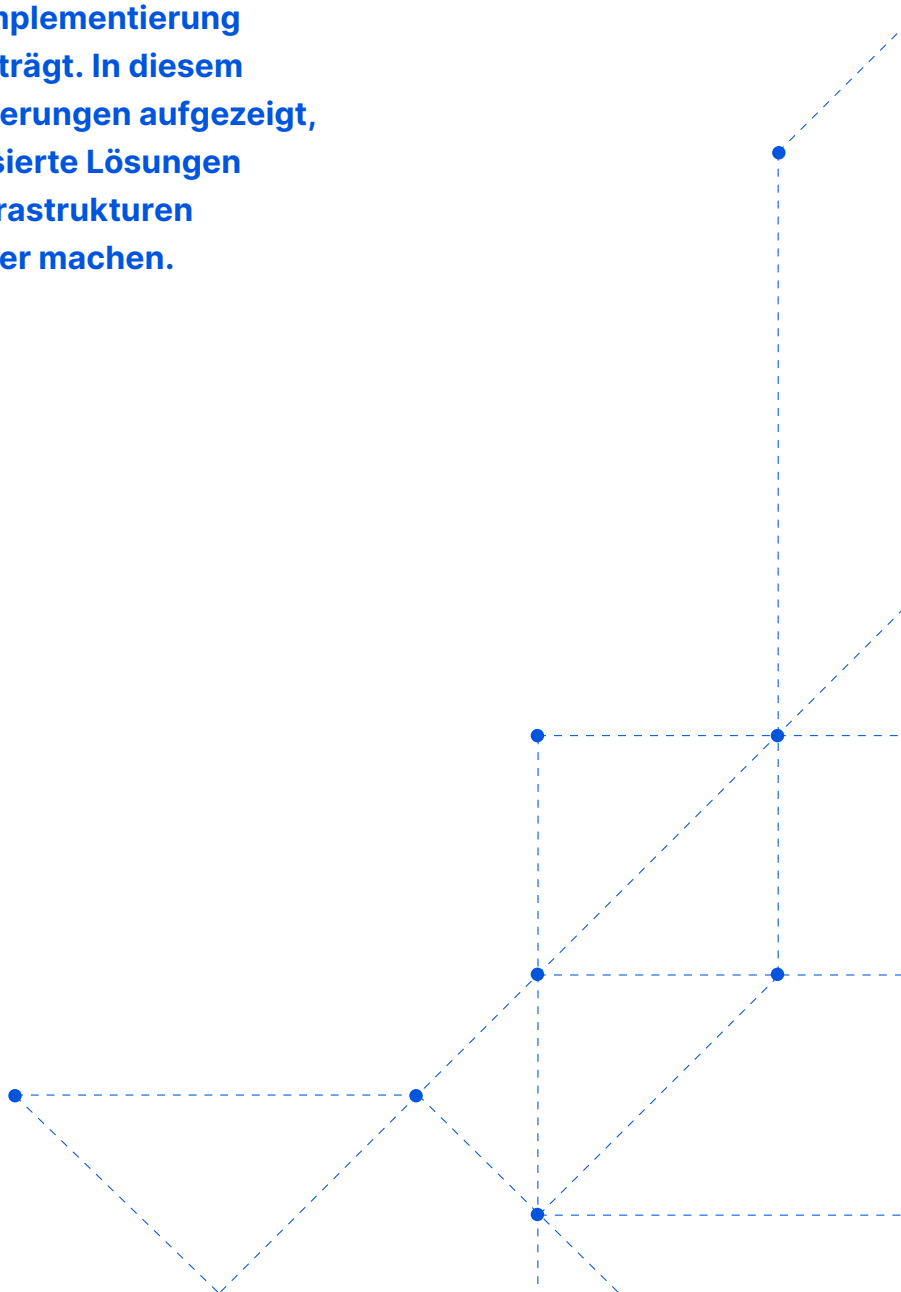
WHITEPAPER

Das Ende hardwarebasierter Netzwerk-Appliances

Warum Sie sich genau jetzt von Netzwerkhardware verabschieden sollten

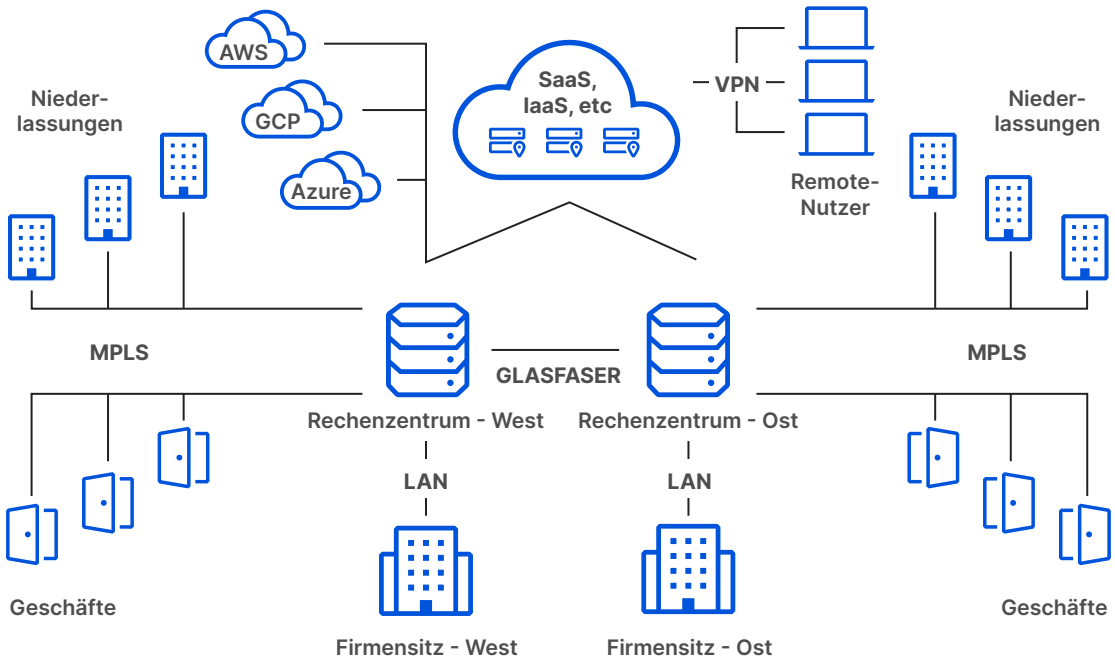
Kurzfassung

Während Storage und Computing in die Cloud verlagert wurden, bleiben viele Netzwerkfunktionen vor Ort. Dies führt zu Kapazitätseinschränkungen, hohen Gesamtbetriebskosten, Herausforderungen beim Support und Sicherheitslücken. Hybrides Arbeiten wird zur Norm. Organisationen kämpfen darum, angemessene Kapazitäten und effektive Sicherheit zu gewährleisten. Viele Transformationsprojekte sind ins Stocken geraten, weil der Rückstand bei der Implementierung neuer Hardware weit über ein Jahr beträgt. In diesem Whitepaper werden diese Herausforderungen aufgezeigt, ihre Folgen quantifiziert und cloudbasierte Lösungen vorgeschlagen, die hybride Cloud-Infrastrukturen schneller, erschwinglicher und sicherer machen.



Einleitung

Die Migration in die Cloud hat sich als effektive Strategie erwiesen, um Infrastrukturkosten zu senken, die Verfügbarkeit von Daten und Anwendungen zu verbessern und die operative Agilität zu erhöhen. Diese Migration erfolgt jedoch selten auf einen Schlag. Viele große Unternehmen verfügen über eine komplexe Mischung aus Multi-Cloud- und On-Premise-Infrastruktur:



Eine solche hybride Infrastruktur ist nicht unbedingt etwas Schlechtes, aber sie bringt Komplikationen mit sich. Insbesondere entstehen Situationen, in denen verschiedene Netzwerkfunktionen wie DDoS-Abwehr, Lastverteilung, Firewall und VPN weiterhin lokal ausgeführt werden.

Veraltete Netzwerk-Hardwaregeräte sind der Aufgabe, kritische Infrastrukturen in einer Cloud-orientierten Welt zu sichern und zu beschleunigen, einfach nicht gewachsen. Sie waren schon immer ein Ärgernis – ein teures, oft unentwirrbares Durcheinander von Geräten und Kabeln. Sobald man dann noch die Cloud ins Spiel bringt, entstehen schnell Sicherheitslücken, Performance-Einbußen und zusätzliche Herausforderungen beim Support.

Das Whitepaper beschreibt die Risiken und Fallstricke bei der Wartung von Netzwerkhardware in einer Welt, in der sich alles in die Cloud verlagert. Zudem bietet es Strategien für den Aufbau eines sicheren und effektiven Netzwerks.

Die Risiken von Hardware in einer Cloud-Welt

Netzwerk-Hardwaregeräte sind für eine Vielzahl spezifischer Funktionen zuständig und werden von Organisation zu Organisation etwas unterschiedlich eingesetzt.

Einige gängige Beispiele:

Sicherheit

- DDoS-Schutz
- Firewall
- Virtuelles privates Netzwerk
- Konfigurierbare Richtlinien

Performance und Zuverlässigkeit

- Lastverteilung
- Traffic-Beschleunigung/ WAN Optimization
- Paketfilterung
- Traffic-Analytics

Wenn diese Hardware lokal eingesetzt wird, entsteht eine Architektur mit diesen fünf Risikokategorien: **Überlastungen der Supply Chain, Kapazitätseinschränkungen, hohe Gesamtbetriebskosten, Supportschwierigkeiten** und **Sicherheitslücken**.

Die ersten drei Kategorien waren schon immer eine Herausforderung selbst für die erfahrensten Netzwerk- und Sicherheitsteams. Die anderen beiden werden durch die Migration in die Cloud noch verschärft.

Überlastungen der Supply Chain

Wie jedes physische Produkt ist auch Netzwerk-Hardware anfällig für eine Vielzahl von Schwierigkeiten in der Supply Chain. Wenn die Materialkosten steigen, bestimmte Materialien und Komponenten schwieriger zu beschaffen sind oder die Versanddienstleister überlastet sind, wird es schwieriger, Netzwerkhardware zu kaufen und zu ersetzen.

Leider sind solche Schwierigkeiten in letzter Zeit häufig geworden. Dies ist zum großen Teil auf die Auswirkungen der Covid-19-Pandemie zurückzuführen. Laut Gartner Research, „waren vor der Pandemie Vorlaufzeiten von 4-6 Wochen üblich. Jetzt sind 200-300 Tage üblich. Wir haben Angebote von Unternehmen gesehen, die gegenüber Kunden eine Vorlaufzeit von über 430 Tagen angegeben haben."

Diese Verzögerungen sind auf mehrere Faktoren zurückzuführen:

- **Schwierigkeiten in der Logistik:** Historische Supply Chain-Modelle weisen mehrere Schwachstellen auf, haben nur ein Minimum an Arbeitskräften und sind in hohem Maße von Technologien abhängig, die mehr oder weniger sicher sind – Herausforderungen, die sich in letzter Zeit deutlich bemerkbar gemacht haben. Während der Pandemie wurden viele Produktionsstätten geschlossen, bei den Spediteuren kam es zu Verzögerungen und viele Arten von Mitarbeitern im Supply Chain-Bereich konnten nur schwer eingestellt und gehalten werden. Aufgrund all dieser Herausforderungen dauert es länger, Hardware herzustellen und zu liefern. Die größte Herausforderung liegt jedoch in der Natur der Logistik, die mit einem Staffellauf vergleichbar ist. Nur weil Ihr eigenes Unternehmen vielleicht keine Probleme hat, bedeutet das nicht, dass Sie nicht von einem defekten Glied weiter oben in der Kette betroffen sind.
- **Höhere Materialkosten:** Netzwerk-Hardware-Appliances sind auf eine Vielzahl von Rohstoffen angewiesen. Aufgrund der hohen Nachfrage und des begrenzten Angebots sind die Materialpreise in die Höhe geschnellt. Das bedeutet, dass Unternehmen nicht nur länger warten müssen, um das zu bekommen, was sie für ihr Netzwerk benötigen, sondern dass sie auch deutlich mehr dafür bezahlen müssen. Leider erwartet Gartner aufgrund dieser Herausforderungen, dass die Vorlaufzeiten für Hardware-Appliances bis Anfang 2023 hoch bleiben werden (Quelle).

All diese Herausforderungen haben Konsequenzen. Wenn Sie sich weiterhin auf die Beschaffung, Wartung und den Austausch von Hardware-Boxen konzentrieren müssen, bedeutet das mehr Gemeinkosten, mehr Zeit für die Planung statt für die Ausführung und zusätzliche Sicherheitsbedenken hinsichtlich der Sicherung einer physischen Supply Chain in unsicheren Zeiten. Anstatt sich auf Logistik, Vorlaufzeiten, Beschaffung und Lagerung von Hardwareboxen zu konzentrieren, könnten sich Unternehmen stattdessen darauf konzentrieren, die Bedürfnisse ihrer Kunden zu erfüllen.

Kapazitätsbeschränkungen

Es sollte keine Überraschung sein, dass Netzwerk-Hardwaregeräte naturgemäß bei unerwartetem Traffic-Anstieg überlastet werden können – unabhängig davon, ob dieser Traffic legitim ist oder nicht. Mehrere Trends der letzten Zeit weisen jedoch darauf hin, dass diese Grenzen immer häufiger erreicht werden.

Denken Sie an die Abwehr von Distributed-Denial-of-Service-Angriffen. Der größte DDoS-Angriff der Geschichte fand Microsoft zufolge im November 2021 statt und soll ein Maximalvolumen von 3,47 Tbit/s erreicht haben (Quelle) DDoS-Angriffe würden die fortschrittlichste DDoS-Abwehr-Hardware auf dem Markt, die in der Regel nur einen Bruchteil der zur Bekämpfung solcher Angriffe erforderlichen Kapazität bietet, um ein Vielfaches überlasten.

Im November 2021 soll der größte DDoS-Angriff der Geschichte ein maximales Volumen von 3,47 Tbit/s erreicht haben.

Nicht alle Unternehmen werden von Angriffen dieses Ausmaßes getroffen – aber auch nicht alle Unternehmen können oder wollen die fortschrittlichste Hardware zur DDoS-Abwehr einsetzen. Ein Cloudflare-Bericht hat ergeben, dass volumetrische Angriffe im Jahr 2022 Q1 zugenommen haben. Tatsächlich wuchsen Angriffe über 10 Mpps (Millionen Pakete pro Sekunde) um mehr als 300 % im Quartalsvergleich, und Angriffe über 100 Gbit/s stiegen im Quartalsvergleich um 645 % (Quelle). Der starke Anstieg der DDoS-Angriffe ist nicht nur alarmierend. Vielmehr würden diese Arten von Angriffen viele vermeintlich leistungsfähige Hardware-basierte Abwehrlösungen überfordern.

Außerdem wird beim Angriffsvolumen nicht der legitime Traffic berücksichtigt, der Ihr Rechenzentrum zur gleichen Zeit erreichen könnte.

Sollte ein kleinerer Angriff während einer Zeit mit hohem Traffic-Aufkommen eintreffen, z. B. während des Einkaufswochenendes am Black Friday, wenn sich die täglichen Seitenaufrufe im E-Commerce-Bereich durchschnittlich über Nacht verdoppeln (Quelle) dann könnte der daraus resultierende Traffic-Anstieg immer noch ausreichen, um die Sicherheitshardware über ihre Belastungsgrenze zu bringen.

DDoS-Abwehr ist nur ein Beispiel für die Kapazitätsbeschränkungen lokaler Hardware.

Hier ein paar weitere Beispiele:

Load Balancer: Einzelne lokale Load Balancer können durch plötzliche Spitzen im legitimen Traffic leicht überlastet werden. Wenn das geschieht, kann es lange dauern, bis zusätzliche Hardware bereitgestellt und installiert ist. Die Alternative besteht darin, genug Kapazität für den schlimmsten möglichen Fall bereitzuhalten, aber dafür müsste die Organisation kontinuierlich eine Menge kostspielige Hardware betreiben.

Virtual Private Networks (VPNs): Die VPN-Nutzung ist viel schwieriger im Voraus zu prognostizieren. Für viele Unternehmen ist vollständig dezentrales und hybrides Arbeiten die neue Normalität, aber der traditionelle VPN-Ansatz erfordert eine sorgfältige Planung, Wartung und Verwaltung, da viele VPNs nicht für die kontinuierliche Nutzung durch ein ganzes Unternehmen konzipiert wurden. Wenn zu viele Mitarbeiter ein VPN nutzen, leiden Konnektivität und Zuverlässigkeit. Außerdem können Sicherheitsprobleme auftreten, da VPNs ohne jegliche Zero Trust-Kontrollen konzipiert wurden. Wenn ein VPN überlastet ist, kann es außerdem vorkommen, dass Unternehmen den Datenverkehr „aufteilen“ (Split-Tunneling), so dass webgebundener Datenverkehr nicht durch das VPN geleitet wird - was die Verfolgung und Verwaltung der Webaktivitäten der Mitarbeiter erschwert.

Angesichts derartiger Probleme sehen manche Unternehmen eine Antwort darin, mehr, neuere und leistungsfähigere Hardware zu kaufen. Ein solcher Ansatz bringt jedoch eine Vielzahl anderer Probleme mit sich.

Betriebskosten

Ähnlich wie das Problem der Kapazitätseinschränkungen sollte es nicht überraschen, dass die Hardware von Rechenzentren teuer ist. Für Hardware mit einer DDoS-Abwehrkapazität von etwa 100 Gbit/s können beispielsweise Anschaffungskosten zwischen 400.000 und 500.000 US-Dollar entstehen.

Und diese Kosten sind nur ein Teil der Gesamtbetriebskosten für die Hardware.

Sehen Sie sich die folgenden Ausgaben an:

- Kosten für das Team: Für Anschaffung, Betrieb und Wartung der Hardware zur Abwehr von Bedrohungen auf allen Layern des OSI-Modells – und zur Bereitstellung des Performance- und Zuverlässigkeitsniveaus, das von modernen Websites und Internetanwendungen erwartet wird – braucht man Experten für jede einzelne dieser Netzwerkfunktionen im Team. Der Aufbau eines Teams mit einem so umfangreichen Fachwissen ist ein kostspieliges Unterfangen – insbesondere in einer Zeit, in der der Arbeitsmarkt so angespannt ist wie nie zuvor. Eine ISACA-Umfrage aus dem Jahr 2022 ergab, dass von 2.000 Cybersecurity-Fachleuten, die an der jährlichen Umfrage teilnahmen, 63 % unbesetzte Stellen im Bereich Cybersecurity haben. Dies stellt einen Anstieg um 8 % gegenüber dem Vorjahr dar (Quelle).
- Instandhaltungskosten: Die durchschnittliche lokale Netzwerkhardware ist nur 3 bis 5 Jahre im Einsatz, wobei oft noch zusätzliche Ausgaben für Garantien für diesen gesamten Zeitraum dazukommen. Wenn Sie das Tempo der technologischen Innovation berücksichtigen, ist es unvermeidlich, dass sich die Lebensdauer dieser vor Ort installierten Geräte weiter verkürzt. Die Alternative sind unerwartete – und damit nicht im Budget vorgesehene – Reparaturen durch den Originalhersteller oder einen Dritten. Hardware-Fehlfunktionen können auch Ausfallzeiten des Rechenzentrums verursachen, was zu durchschnittlichen Opportunitätskosten von über 8.800 US-Dollar pro Minute führt (Quelle).
- Austauschkosten: Um ein Hardwaregerät alle drei Jahre zu ersetzen, müssen Unternehmen nicht nur erneut den Betrag der Anfangsinvestition ausgeben, sondern auch Ressourcen für den Versand und die Installation der neuen Hardware aufwenden. Eine Verzögerung dieser Austauschvorgänge führt oft zu häufigeren Fehlfunktionen – und damit zu zusätzlichen Instandhaltungskosten.

Vergleichen Sie dieses Modell mit Cloud-basierten Netzwerkdiensten. Dabei kann mit einem flexibleren Team gearbeitet werden, es entstehen keine Unterhalts- und Versandkosten, und Organisationen werden nicht gezwungen, zwischen kostspieligen Upgrades und zunehmenden Fehlfunktionen zu wählen.

Hardware-Fehlfunktionen können Ausfallzeiten des Rechenzentrums verursachen, was zu durchschnittlichen Opportunitätskosten von über 8.800 US-Dollar pro Minute führt.

Herausforderungen beim Support

Support von Netzwerk-Hardwaregeräten ist nicht nur ein teures Unterfangen, sondern auch eine logistische Herausforderung. Hardware muss häufig gepatcht werden, um mit den neuesten Sicherheitsrisiken und Angriffstaktiken Schritt halten zu können – ein Prozess, der oft auf einer manuellen Implementierung beruht und daher anfällig für menschliche Fehler ist.

Je mehr Hardware-Geräte eine Organisation einsetzt, desto größer ist die Wahrscheinlichkeit, dass sie aus Unachtsamkeit oder aus Sorge um die Beeinträchtigung wichtiger Systeme einen Patch vernachlässigt. In einem kürzlich veröffentlichten gemeinsamen Cybersecurity Advisory haben die National Security Agency (NSA), die Cybersecurity and Infrastructure Agency (CISA) und das Federal Bureau of Investigations (FBI) berichtet, dass 16 öffentlich bekannte Sicherheitslücken in ungepatchten Netzwerkgeräten in breit angelegten Kampagnen ausgenutzt wurden (Quelle). Die Schwachstellen betreffen verschiedene Geräte vor Ort, von Routern für kleine Unternehmen bis hin zu Firmen-VPNs, und geben den Angreifern potenziell die Möglichkeit, den Netzwerk-Traffic zu manipulieren und Daten aus den Zielnetzwerken zu exfiltrieren.

Auch wenn die meisten der 16 aufgelisteten Sicherheitslücken als kritisch eingestuft werden, ist das Patchen und die Behebung keine einfache Aufgabe. Tatsächlich kann das Patchen von Hardware so komplex sein, dass es eine ganze Kategorie von Software gibt, die Unternehmen dabei hilft, auf dem neuesten Stand zu bleiben (Quelle).

Und die Folgen eines einzigen versäumten Patches können erheblich sein. Die Hardware bleibt nicht nur anfällig. Sobald ein Patch veröffentlicht wird, wird die entsprechende Schwachstelle zu einem höherwertigen Ziel für opportunistische Angreifer. Vergleichen Sie diese Situation mit Cloud-basierten Sicherheitsdiensten, bei denen die Behebung von Schwachstellen und die Installation von Updates standardmäßig automatisch erfolgt und je nach Netzwerkgeschwindigkeit des Cloud-Providers in lediglich dreißig Sekunden realisiert werden kann.

Weitere Herausforderungen bei der Wartung von Hardware sind:

- **Fehlerbehebung:** In einem reinen Hardware-Szenario müssen IT-Teams bei der Fehlerbehebung oft einen mühsamen Prozess durchlaufen, bei dem Load Balancer, Firewalls und andere On-Premise-Geräte nacheinander abgeschaltet werden, um herauszufinden, wo das Problem liegt.

  Dieser Prozess wird durch die Nutzung von Cloud-Diensten zusätzlich erschwert. Unternehmen verwalten den Zugang zu diesen Diensten häufig über das zentrale Rechenzentrum und alle seine einzelnen Geräte. Wenn Mitarbeiter nicht auf einen bestimmten Dienst zugreifen können, müssen IT-Teams eine weitere Stelle überprüfen, um die Probleme zu diagnostizieren. Berücksichtigt man einen aktuellen Bericht von Productiv, aus dem hervorgeht, dass 56 % aller SaaS-Anwendungen unter die Kategorie der Schatten-IT fallen – oder nicht genehmigte und nicht verwaltete Anwendungen, die ohne Wissen der IT-Abteilung beschafft werden –, dann wird dieses Problem sowohl in seinem Umfang als auch in seinem Ausmaß schnell größer (Quelle).
- **Physische Wartung:** Wenn ein Hardwaregerät kaputt geht, müssen IT-Teams den Stecker physisch herausziehen, Ersatz bestellen, den Ersatz testen und neu installieren – ein weiterer mühsamer Prozess. Wenn man die Größe vieler globaler Unternehmen bedenkt, könnten sich die zu wartenden Geräte am anderen Ende der Welt befinden.

Sicherheitslücken

Selbst wenn eine Organisation über die Ressourcen verfügen würde, die für die kontinuierliche Bereitstellung und Wartung der neuesten und leistungsfähigsten On-Premise-Hardware erforderlich sind, würde die daraus resultierende Infrastruktur immer noch unter kritischen Sicherheitsmängeln leiden – insbesondere in einer Welt, in der der Trend zur Cloud geht.

Denken Sie an die Verwaltung des Mitarbeiterzugriffs. VPN-Hardware kann zwar verschlüsselte Tunnel zwischen Geräten von Remote-Mitarbeitern und Anwendungen einrichten, die in einem internen Rechenzentrum gehostet werden, aber sie kann die Benutzeraktivitäten nach der Einrichtung dieses Tunnels nicht überwachen und sichern.

Sollte das Gerät eines Mitarbeiters durch Malware kompromittiert werden oder ein Phishing-Angriff seine VPN-Anmeldedaten kompromittieren, könnte ein Angreifer über diesen VPN-Zugang an eine Vielzahl sensibler Informationen gelangen. Sowohl Phishing als auch Malware stellen nach wie vor ernsthafte Risiken dar und bringen Bedrohungsakteuren erhebliche finanzielle Gewinne ein. Im Jahr 2021 gingen dem FBI zufolge 6,9 Milliarden Dollar durch Cyberkriminalität verloren. Insbesondere die Kompromittierung von Geschäfts-E-Mails (Business Email Compromise – BEC) kostete Unternehmen 2,4 Milliarden Dollar an Verlusten. (Quelle).

Sollte das Gerät eines Mitarbeiters durch Malware kompromittiert werden oder sollte ein Phishing-Angriff die VPN-Zugangsdaten des Mitarbeiters kompromittieren, könnte ein Angreifer über diesen VPN-Zugang an eine Vielzahl sensibler Informationen gelangen.

Cloud-Dienste und SaaS-Anwendungen erschweren die Sicherheit einer hardware-zentrierten Infrastruktur zusätzlich. In einem hybriden Cloud-Modell betreibt ein Unternehmen beispielsweise eine Mischung aus lokaler und Cloud-Infrastruktur. Das Unternehmen kann Sicherheitshardware nicht einfach an einen Cloud-Anbieter senden. Wenn das Unternehmen weiterhin Hardware vor Ort für sein eigenes Rechenzentrum verwenden möchte, werden die verschiedenen Teile seiner Infrastruktur auf unterschiedliche Weise geschützt, wodurch die Sicherheitsteams weniger Einblick in und Kontrolle über eingehende Angriffe haben.

Cloudbasierte Dienste können diese beiden Herausforderungen überwinden. Dazu vereinen sie Rechenzentren und Clouddienste unter einem einzigen softwaredefinierten Layer.

Eine detaillierte Erklärung dieses Ansatzes würde den Rahmen dieser Abhandlung sprengen. In den folgenden Artikeln können Sie mehr darüber lesen:

- Was ist ein Zero-Trust-Netzwerk?
- Was ist Secure Access Service Edge?

Cloud-basierte Sicherheits- und Performancedienste: Vorteile und Herausforderungen

Die Bereitstellung von Netzwerkdiensten über die Cloud vermeidet viele der Probleme, die mit Hardware verbunden sind: Überlastungen der Supply Chain, Kapazitätseinschränkungen, Kosten, Supportprobleme und Sicherheitslücken.

- **Supply Chain:** Viele cloudbasierte Netzwerkanbieter sind darauf ausgelegt, mit modernen, globalen Architekturen zu skalieren, wodurch Probleme in der Supply Chain weniger akut werden.
- **Kapazität:** Aufgrund des verteilten und Software-definierten Charakters der Cloud können Unternehmen zusätzliche Kapazitäten problemlos bereitstellen, wenn ihr Geschäft wächst.
- **Kosten:** Die zusätzlichen Kosten für Hardware sind entweder nicht existent oder im Voraus leichter zu planen. Hinzu kommt, dass Cloud-Dienste in der Regel als Betriebsausgaben und nicht als Investitionsausgaben eingestuft werden, was für viele Unternehmen steuerliche und buchhalterische Vorteile bietet.
- **Support:** Die logistischen Anforderungen und der Ressourcenbedarf werden vom Dienstanbieter gedeckt. Darüber hinaus gibt es keine Möglichkeit, einen Patch zu verpassen, da Aktualisierungen automatisch erfolgen.
- **Sicherheit:** Software-definierte Netzwerkdienste können verschiedene Infrastrukturen unter einer einzigen Schutzschicht vereinen.

Allerdings bergen Cloud-Netzwerkdienste ihre eigenen Risiken, wenn sie nicht mit Bedacht eingesetzt werden:

Risiko	Beschreibung
Latenz	Einige cloudbasierte Netzwerkfunktionen sind auf spezialisierte cloud-basierte Rechenzentren angewiesen – z.B. Scrubbing-Zentren zur DDoS-Abwehr. Das Backhauling des Datenverkehrs zu diesen Rechenzentren kann je nach Standort relativ zum Zielserver zu erheblichen Latenzzeiten führen. Dieses Problem verschärft sich, wenn ein Unternehmen verschiedene Anbieter für unterschiedliche Netzwerkfunktionen nutzt. Wenn der Datenverkehr von Provider zu Provider springen muss, kann die Latenz in Hunderten von Millisekunden gemessen werden.
Support	Wenn eine Organisation verschiedene Provider für verschiedene Funktionen einsetzt, bleibt die Fehlerbehebung weiterhin ein Problem. Manchmal ist es schwer zu sagen, welcher Provider die Ursache für Verstopfung oder Ausfälle ist.
Kosten	Wenn eine Organisation verschiedene Provider für verschiedene Funktionen einsetzt, kann der Zeitaufwand (und damit die Kosten) für deren Verwaltung immer noch hoch sein.

Um diese Probleme zu vermeiden, sollten Sie die folgenden Strategien in Betracht ziehen:

- **Suchen Sie nach Providern, die sowohl mit Cloud- als auch mit On-Premise-Infrastrukturen arbeiten.**
  Dadurch können IT- und Sicherheitsteams von einem einzigen Ort aus einheitliche Kontrollen einrichten und den globalen Traffic überwachen. Es hilft auch, eine widerstandsfähigere Architektur aufzubauen – eine Architektur, mit der Ihre Teams schnell auf Schwankungen der Marktbedingungen reagieren können.
- **Suchen Sie nach Cloud-Providern, die mehrere Netzwerkfunktionen anbieten, die zusammenarbeiten.**
  Dadurch wird häufig die Anzahl der Netzwerk-Hops reduziert, die der Traffic ausführen muss, was zu niedrigerer Latenz und damit zu einer besseren Erfahrung für den Endbenutzer führt. Auch die Behebung von Netzwerkproblemen ist einfacher, wenn Sie sich an ein einziges Unternehmen statt an viele wenden müssen. Außerdem führt die Bündelung mehrerer Funktionen oft zu niedrigeren Kosten.
- **Suchen Sie nach Cloud-Providern, die von jedem Standort in ihrem Netzwerk mehrere Netzwerkfunktionen ausführen können.**
  Provider, die ihr Service-Portfolio durch Übernahmen erweitern, binden neue Dienste nicht immer vollständig ein, was bedeutet, dass bestimmte Funktionen nur über bestimmte Rechenzentren bereitgestellt werden können. Ziehen Sie Provider in Betracht, die diese Funktionen in ihrem gesamten Netzwerk anbieten, um die oben genannten Probleme zu vermeiden.
- **Suchen Sie nach Cloud-Providern mit umfangreicher globaler Präsenz.**
  Dadurch wird der vorherige Punkt unterstützt und es wird sichergestellt, dass Endbenutzer immer in der Nähe des Netzwerks sind, egal wo sie sich befinden. Außerdem wird eine große Netzwerkoberfläche geschaffen, mit der DDoS-Traffic absorbiert und andere Netzwerkfunktionen durchgeführt werden können, die eine große Kapazität erfordern.

Der Nutzen von Cloudflare

Wie können Unternehmen ihre Netzwerktransformation beschleunigen, ohne auf die Lieferung von Hardware zu warten und ohne noch mehr Geld in Boxen zu stecken, die nur ein paar Jahre halten werden?Mit Cloudflare.

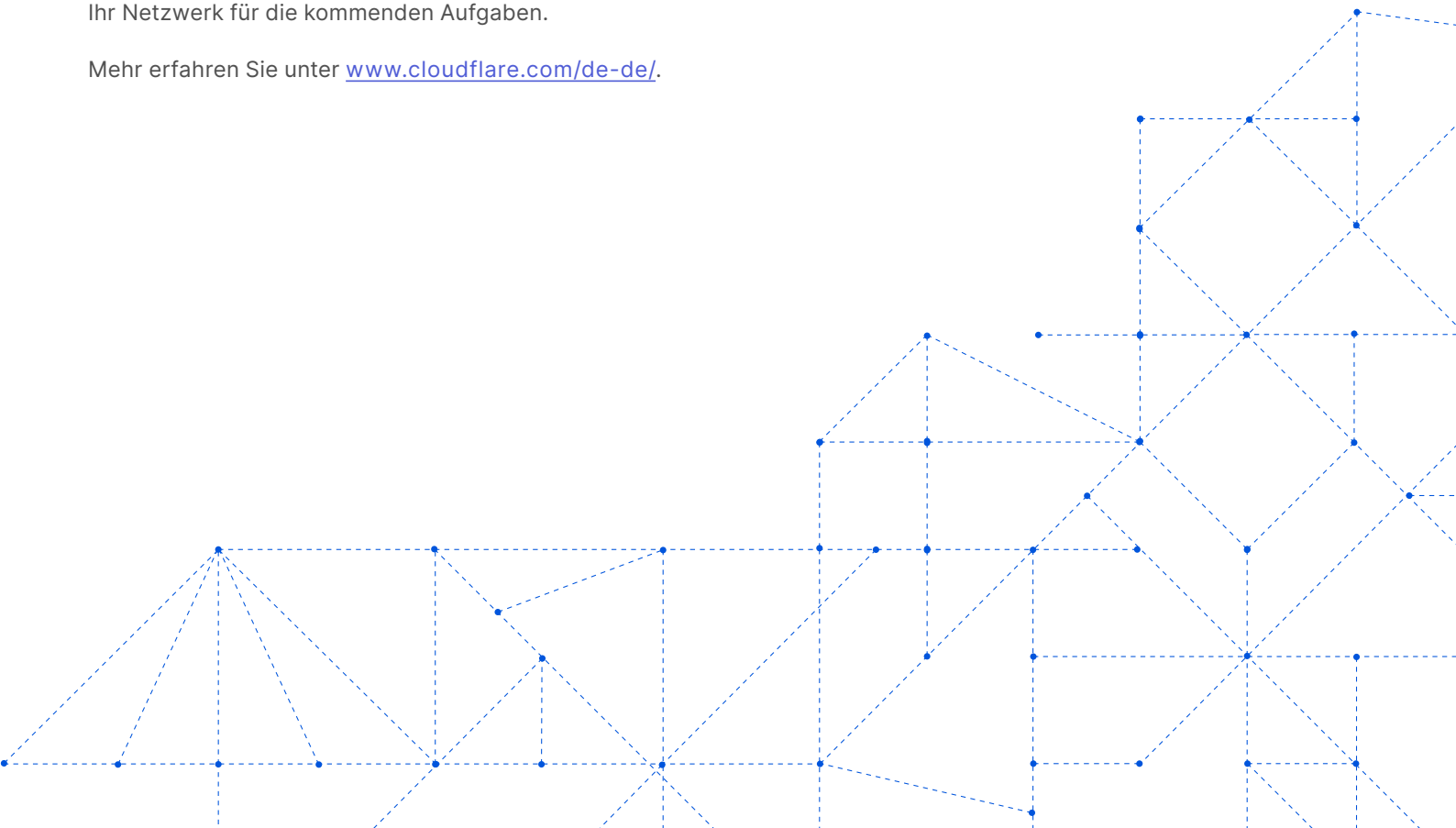
Cloudflare hat eine globale Cloud-Plattform aufgebaut, die eine breite Palette an Diensten bereitstellt – sie macht Unternehmen sicherer, verbessert die Performance ihrer Anwendungen und eliminiert die Kosten und die Komplexität, die bei der Verwaltung einzelner Netzwerk-Hardware anfallen. Diese Plattform dient als skalierbare, benutzerfreundliche, einheitliche Kontrollebene für Sicherheit, Performance und Zuverlässigkeit für On-Premise-, Hybrid-, Cloud- und SaaS-Anwendungen (Software-as-a-Service).

Entscheidend ist, dass jedes Rechenzentrum in Cloudflares weltweitem Netzwerk mit über 270 Städten jeden dieser Dienste bereitstellen kann, wodurch die Latenz reduziert wird, die Cloud-Implementierungen erschweren kann. Optimieren Sie Ihren Netzwerk-Stack, beschleunigen Sie die Transformation und wappnen Sie Ihr Netzwerk für die kommenden Aufgaben.

Mehr erfahren Sie unter www.cloudflare.com/de-de/.

„Dropbox ist seit kurzem ein „Virtual First“-Unternehmen. Wir haben untersucht, wie sich diese Geschäftsstrategie auf unseren Sicherheitsansatz und unsere Netzwerkarchitektur auswirkt. Wir schätzen die Unterstützung von Cloudflare, die uns und anderen Remote-First-Organisationen wie der unseren dabei hilft, sich an diese „neue Normalität“ anzupassen.“

Konstantin Sinichkin
Engineering Manager, Dropbox



+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

REV:BDES-3313.2022JUN10