ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Oktober 2019

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Konsolidierung im Rechenzentrum weitergedacht – Converged und Hyperconverged Infrastructure

von Dr. Markus Ermes und Cornelius Höchel-Winter

Automation und Betriebsoptimierung sind die großen Themen in unseren Rechenzentren. Der erste wichtige Schritt war die Virtualisierung von Servern. Um die beiden anderen Bereiche Storage und Netzwerk ebenfalls auf eine virtualisierte Ebene zu heben, stehen mittlerweile seitens der Hypervisor-Hersteller leistungsfähige Tools zur Verfügung. Damit ist das sogenannte Software-defined Datacenter (SDDC) in greifbarer Nähe. Was ist aber mit der zugrunde liegenden Hardware?

Ja, die Hersteller von Servern oder Netzwerkkomponenten bieten Verwaltungswerkzeuge für **ihre** Produkte an, aber letztlich wird damit die Silostruktur vieler Betriebsorganisationen nur weiter zementiert, statt – im Sinne der anwendungsorientierten Gesamtsteuerung des SDDC – die strikte Trennung aufzuweichen und zu mehr Zusammenarbeit zu kommen. Sogenannte Converged- und Hyperconverged-Lösungen versprechen hier Abhilfe: Integrierte und vorkonfigurierte Gesamtkonzepte für Compute, Storage und Netzwerk aus einer Hand. Doch nicht jede Lösung ist für jedes Umfeld geeignet. Wir geben in diesem Artikel einen Überblick über CI- und HCI-Lösungen und zeigen beispielhaft, wo Einsparungen und Betriebsoptimierungen liegen können.

weiter auf Seite 8

Web Security aus der Cloud: Eine langfristige Option oder experimenteller Hype?

von Timo Schmitz

Die Absicherung des Internetzugriffs für Mitarbeiter eines Unternehmens nimmt einen hohen Stellenwert in der Informationssicherheit ein. Dazu verfolgen verschiedene Appliances das Ziel, den Nachrichtenverkehr auf Schadcode zu inspizieren bzw. dafür zu sorgen, dass unternehmensweite Richtlinien wie verweigerte Zugriffe auf verbotenen Webseiten durchgesetzt werden.

In den vergangenen Jahren etablierten sich hierzu Lösungen, die auf einer Cloud-Infrastruktur aufsetzen und dem Unternehmen verschiedene Vorteile finanzieller und technischer Natur versprechen. Ob solche Lösungen ein innovativer Schritt Richtung Zukunft sind oder sich der Trend womöglich als „Eintagsfliege“ herausstellen könnte, soll in diesem Artikel besprochen werden. Zusätzlich werden Schritte vorgestellt, die bei der Einführung einer solchen Lösung aus der Cloud beachtet werden sollten.

weiter auf Seite 24

Geleit

Cloud First – und dann?

In vielen Unternehmen gibt es mittlerweile die Vorgabe „Cloud First“. Dies bedeutet, dass zumindest bei jeder Neuentwicklung bzw. Neuplanung die Cloud bevorzugt wird. Unabhängig von der Sinnfälligkeit einer solchen Vorgabe muss eine Reihe von Fragen geklärt werden. Um welche Fragen geht es? Was sind die Antworten darauf?

In meinem letzten Geleit [1] plädierte ich dafür, Cloud Computing geregelt zu nutzen und nichts dem Zufall zu überlassen. Anlass war meine Feststellung, dass die Entwicklung und Planung für die Cloud in einigen Unternehmen ein Eigenleben entwickelt hat. Dieses Eigenleben kann zu einer dualen IT führen, mit anderen Regeln als die IT-Umgebungen „on premises“ (OnPrem), also im eigenen Rechenzentrum. Dafür habe ich die Beispiele Zonenkonzept und Perimeter genannt. Hier möchte ich auf ein paar andere Themen im Zusammenhang mit der Cloud-Nutzung eingehen.

Bleibe ich der uneingeschränkte Herrscher über meine Daten?

Diejenigen, die sich in der eigenen IT-Infrastruktur mit der Sicherung und Wiederherstellung von Daten befasst haben, wissen, dass es dabei sehr komplexe Probleme geben kann. Mit der Cloud kommen neue Probleme dazu.

Der Klassiker, der jede Organisation betreffen kann, ist die Herrschaft über die Daten im Zusammenhang mit Kommunikation und Teamarbeit.

Seit Jahrzehnten nutze ich die Kombination aus einer strukturierten Dateiablage und E-Mails, die ich ebenfalls strukturiert aufbewahre. So war ich neulich in der Lage, die Historie der Zuweisung unseres IP-Adressraums anhand von E-Mails aus den 1990er Jahren nachzuvollziehen. An dieser Stelle habe ich nicht vor, auf die Nachteile meines sicher persönlich geprägten Datenmanagements einzugehen (etwa auf die Schwierigkeiten, die meine Kollegen mit meinen Datenablagen haben werden, sollte ich plötzlich ausfallen und auch nicht ansprechbar sein). Fakt ist, dass sich heute meine Daten nicht mehr ausschließlich in Dateien, E-Mails und On-Prem-Datenbanken befinden. Im Zusammenhang mit der Organisation von Seminaren, Kongressen und anderen

Veranstaltungen der ComConsult Akademie werden Daten generiert, die nur zum Teil als Dateien vorliegen. Zum Beispiel wird einiges in Chats abgestimmt. Da Kommunikation und Teamarbeit zunehmend in der Cloud stattfinden, landen die Chat-Daten dort.

Die Fragen bezüglich Datensicherheit und Datenschutz möchte ich an dieser Stelle ausklammern, wie wichtig sie auch sind. Eine andere Frage ist ebenso wichtig, nämlich die Frage nach der uneingeschränkten Kontrolle über die Daten. Meine E-Mails liegen in uns wohl bekannten und von uns beherrschten Ablagen. In diesen Ablagen finde ich notfalls 30 Jahre alte Daten. Sie sind mehrfach gesichert und von einzelnen Speichermedien sowie einzelnen Speicherorten unabhängig. Gilt das auch für die Chat-Daten?

Die unangenehme Antwort auf diese Frage ist ein klares Nein. Wer zum Beispiel Microsoft Teams nutzt, muss zumindest bisher damit rechnen, dass die Chat-Daten nicht einfach aus der Microsoft Cloud exportiert werden können. Der Kunde ist damit kein uneingeschränkter Herrscher über seine Daten. Kann ich darauf setzen, dass meine Nachfolger*innen in 30 Jahren nachvollziehen können, was ich heute in Chats vereinbare? Nein. Verbindliches mit solch langer Wirkung muss ich anderweitig dokumentieren. Niemand kann garantieren, dass es die Microsoft Cloud in 30 Jahren noch gibt.

Sind Cloud-Kosten beherrschbar?

Die Motivation vieler Unternehmen für die Cloud-Nutzung ist die Wirtschaftlichkeit. Wir müssen jedoch immer wieder feststellen, dass die Entscheidung für die Cloud nicht auf Basis einer vollständigen Kostenbetrachtung erfolgt. Wenn eine OnPrem-Applikation durch eine Cloud-Anwendung ersetzt wird, müssen wir die Kosten für den Zugang zur Cloud berücksichtigen. Uns bekannte Unternehmen erhöhen dafür die Bitrate ihres Internet-Zugangs in signifikantem Maße. Aber auch die Rechnung, die ich vom Cloud-Betreiber bekomme, kann sehr hoch ausfallen. Die Preismodelle in Clouds können durchaus komplex und unübersichtlich sein. Die Kette aus Speicherung, Verarbeitung und Übertragung von Daten in der Cloud verursacht an verschiedenen Stellen Kosten. Auf den ersten Blick scheinen diese Kosten geringfügig zu sein, weil sie oft feingranular pro GB und Stunde angegeben werden. Aber das Jahr hat 8760 Stunden, und meine Datenmengen können hunderte bis tausende Gigabytes groß sein!

Kostenkontrolle ist für die Cloud anders als OnPrem. Wir kennen die Kostenkomponenten in der eigenen IT-Infrastruktur ziemlich gut. Eine Berechnung der Total Cost of Ownership (TCO) einer Lösung im eigenen RZ ist nicht trivial. Aber darin sind wir geübt. Wir haben Erfahrung in der Schätzung und Feststellung von Kosten für Hardware, Service, Lizenzen, Raummiete, Kühlung, Energie, Betrieb etc. Nun müssen wir wissen, was ein virtueller Prozessor in der Cloud jährlich kostet, wie viel wir auf welchem Cloud-Speicher pro MB und Jahr bezahlen müssen, welche Kosten ein Internet Gateway in der Cloud verursacht, wie teuer die Datenübertragung zwischen verschiedenen Cloud-Regionen ist usw. Eine wichtige Übung jedes Ingenieurs ist die Kostenschätzung. Darin sind wir, was die Cloud betrifft, noch kaum geübt.

Umso wichtiger ist eine Kostenkontrolle im engen Zeitraster, zumindest täglich. Wir kennen Kostenbremsen zum Beispiel bei der Mobilfunknutzung. Habe ich mein monatliches Datenkontingent aufgebraucht, surfe ich bis zum Monatsende mit angezogener Handbremse. Solche Mechanismen sind in der Cloud entweder nicht verfügbar oder nicht gewünscht. Um böse Überraschungen zu vermeiden, muss man häufig in die Kostenübersicht der Cloud-Konsole hineinschauen. Stelle ich explodierende Kosten fest, muss ich auch noch schnell herausfinden, auf welche Änderung die steigenden Kosten zurückzuführen sind.

Konsolidierung im Rechenzentrum weitergedacht – Converged und Hyperconverged Infrastructure

Fortsetzung von Seite 1

Dr. Markus Ermes hat im Bereich der optischen Simulationen promoviert und Artikel in verschiedenen Fachzeitschriften veröffentlicht. Teil seiner Promotion waren Planung, Aufbau und Nutzung von verteilten und Höchstleistungs-Rechenclustern (HPC). Bei der ComConsult GmbH berät er Kunden im Bereich Rechenzentren, wobei seine Hauptaufgaben bei Netzwerken, Storage und Cloud-basierten Diensten liegen. Seine Kenntnisse im HPC-Bereich geben zusätzlich Einblicke in modernste Hochleistungstechnologien (CPU, Storage, Netzwerke), die in Zukunft auch im Rechenzentrum Einzug halten können.

Cornelius Höchel-Winter arbeitet als Senior-Consultant, Autor, Trainer und Referent auf Seminaren und Kongressen seit 2001 für die ComConsult Firmengruppe. Schwerpunkte seiner Tätigkeit sind die Bereiche Data Center, Virtualisierung, Storage, Netzwerke, Cloud Computing und Systemintegration sowie Evaluierungen neuester Hard- und Softwareprodukte und die Beobachtung aktueller Entwicklungen im IT-Markt. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von RZ- und Campusnetzen und von Windows- und Linux-Umgebungen.

Wenn man RZ-Betreiber fragt, welcher Wunsch ihnen am meisten unter den Nägeln brennt, dann hört man in der Regel drei Forderungen:

Hardwareunabhängigkeit, Automation, niedrigere Betriebskosten.

Nun sind RZ-Betreiber keine Träumer, die irgendwelche Phantastereien äußern. Die meisten wissen genau wovon sie reden, denn sie haben eine Technologie vor Augen, die sie selbst in den letzten Jahren umgesetzt haben und die genau diese Erwartungen realisiert hat: die Virtualisierung von Servern.

Virtualisierung ist erfolgreich

Servervirtualisierung ist letztlich deshalb so erfolgreich, weil mit dieser Technologie sehr konsequent das generelle Konzept „Virtualisierung“ umgesetzt wurde:

- Einführung einer Abstraktionsebene, die die physische Welt möglichst vollständig von der virtuellen Welt trennt: Das Betriebssystem und die Anwendungen auf den virtuellen Maschinen „wissen“ nicht, dass sie sich in einer virtuellen Welt befinden.
- Nachbildung von physischen Ressourcen durch Software im virtuellen Umfeld: Hierbei werden jedoch zum einen nur die Ressourcen nachgebildet, die für die gewünschten Dienste - hier also für den Betrieb eines x86-Servers - notwendig sind. Zum anderen werden die Ressourcen vereinfacht nachgebildet. Auf Spezialitäten aus der physischen Welt, die nur hier gebraucht werden, wird bei ihren virtualisierten Pendants verzichtet – so sind virtuelle Netzwerkkarten beispielsweise nicht auf eine bestimmte Bandbreite resp. Durchsatzleistung festgelegt.
- Möglichkeit zur Bildung von Ressourcenpools: Virtualisierte Ressourcen können ein und derselben physischen Ressource zugeordnet werden.

Die Abstraktionsschicht garantiert Hardwareunabhängigkeit. Die Abbildung von Hardware auf Softwarekonstrukte gestattet Automation, und Automation bedeutet schnelle Bereitstellung, d.h. schnelles und flexibles Reagieren auf Anforderungen aus dem Betrieb. Und nicht zuletzt ermöglichen Ressourcenpools eine bessere Auslastung der physischen Server. Alles zusammen vereinfacht Virtualisierung den Betrieb und eröffnet damit zumindest das Potential, Betriebskosten zu reduzieren – auch wenn dies erfahrungsgemäß keine unmittelbare Folge von Virtualisierung ist.

Klingt gut. Ist es auch! Aber sind wir damit bereits am Ziel? Bekanntermaßen nicht.

Virtualisierung ist nicht alles

Aus Sicht der Virtualisierung fehlen zunächst einmal noch die beiden anderen großen Ressourcenblöcke Netzwerk und Speicher, und zur übergreifenden Automatisierung des Rechenzentrums – je nach Blickwinkel meist mit den Begriffen Software-Defined Data Center (SDDC) oder auch Private Cloud belegt – noch eine zusammenfassende Orchestrierungsschicht.

Die Integration von Speicher ist hierbei vom Grundsatz gar nicht so komplex. Auf der einen Seite besitzen die Hypervisor selbst bereits eine Abstraktionsschicht für Serverspeicher, über die sie ihren virtuellen Maschinen virtuelle Festplatten aus praktisch beliebigen Quellen zur Verfügung stellen. Auf der anderen Seite sind die klassischen Storage-Kon-

Konsolidierung im Rechenzentrum weitergedacht – Converged und Hyperconverged Infrastructure

zepte wie NAS (Network Attached Storage) und SAN (Storage Area Network) ihrerseits bereits so etwas wie Virtualisierungsschichten, die den Zugriff auf den physischen Speicher in Form von Verzeichnisstrukturen oder logischen Bereichen von Speicherblöcken (LUN - Logical Unit Number) bereitstellen.

Im Bereich Netzwerk hat es etwas länger gedauert, bis die Konzepte fertig waren. Aber auch hier stehen mittlerweile Produkte (zum Beispiel VMware NSX) zur Verfügung, um sowohl den Netzwerkverkehr zwischen virtuellen Maschinen als auch Netzwerkdienste wie Routing, Load Balancing, Firewalling etc. unabhängig vom zugrunde liegenden physischen Netz auf eine virtuelle Ebene zu heben.

Im Fokus dieser Technologien steht die Bereitstellung von Anwendungen, mithin also die unmittelbare Unterstützung von Geschäftsprozessen – zweifellos eine, wenn nicht die Kernaufgabe für RZ-Betreiber. Dass in einem Rechenzentrum daneben noch ein paar mehr Kleinigkeiten bereitgestellt werden, wird in diesen Konzepten oft außer Acht gelassen, spielt aber auch im Folgenden keine große Rolle. Wir wollen vielmehr diskutieren, warum Virtualisierung nicht alle Probleme löst, und mit Converged und Hyperconverged Infrastructure ergänzende Konzepte für moderne Rechenzentren untersuchen.

Was bedeutet Converged Infrastructure?

Die Hypervisor-Hersteller haben mit dem beschriebenen Konzept Virtualisierung und der damit verbundenen Hardware-Unabhängigkeit die Hardware-Hersteller massiv unter Druck gesetzt. Plötzlich ist es gar nicht mehr wichtig, ob der neue Virtualisierungshost von Dell, HP, Fujitsu oder einem anderen Hersteller kommt. Lediglich die Prozessorarchitektur spielt innerhalb eines Virtualisierungsclusters noch eine Rolle, um Funktionen wie vMotion oder Live Migration nutzen zu können.

Die Wahrheit ist jedoch, dass die Hypervisor zwar eine Reihe von Hardware-Merkmalen durch Abstraktion verbergen und virtuelle Maschinen problemlos vom Server des Herstellers A auf einen Server des Herstellers B verschoben werden können, dass aber Hardware-Unabhängigkeit natürlich nicht „ohne Hardware“ bedeutet. Und physische Virtualisierungshosts müssen eben auch betrieben werden, genauso wie der notwendige physische Storage und die physischen Netze dazwischen – und zwar zusätzlich zu allen virtuellen Ressourcen und zur Virtualisierungsebene.

Hier setzen Konzepte wie Converged Infrastructure (CI) und Hyperconverged Infrastructure (HCI) an.

Die Zielrichtung bei Converged und Hyperconverged Infrastructure ist zunächst ebenfalls der Betrieb. Genau wie bei Virtualisierung soll der Betrieb im Rechenzentrum einfacher, effektiver und schneller werden. CI und HCI richten sich an Kunden, die Betrieb und Wartung konsolidieren möchten und - statt Hardware von unterschiedlichen Herstellern zu beziehen -auf integrierte Lösungen nur eines Anbieters „für alles“ setzen. Wobei in diesem Zusammenhang „ein Anbieter“ nicht notwendigerweise „ein einziger Hersteller“ bedeutet!

Der Ansatz bei Converged Infrastructure ist, geeignete, vorqualifizierte Hardware-“Bausteine” für Compute, Netzwerk und Speicher meist in einem vorkonfigurierten Chassis oder Rack als Gesamtpaket gebrauchsfertig, also quasi schlüsselfertig an die Kunden auszuliefern. Ergänzt werden diese Hardware-Pakete in der Regel durch

- passende Hardware-, Software- und Verwaltungstools zur Konfiguration, Überwachung und Administration des Gesamtsystems und aller aktiven und passiven Komponenten,
- optional auch durch entsprechende Services des Herstellers beziehungsweise Lieferanten und
- falls gewünscht, meist ebenfalls vorkonfigurierte System- und Anwendungssoftware wie Hypervisor, Datenbanksysteme etc.

Da kommt auch die Bezeichnung „Data Center in a Box“ her: Der Kunde bekommt ein abgestimmtes integriertes Gesamtpaket, das sehr einfach und schnell in Betrieb genommen werden kann.

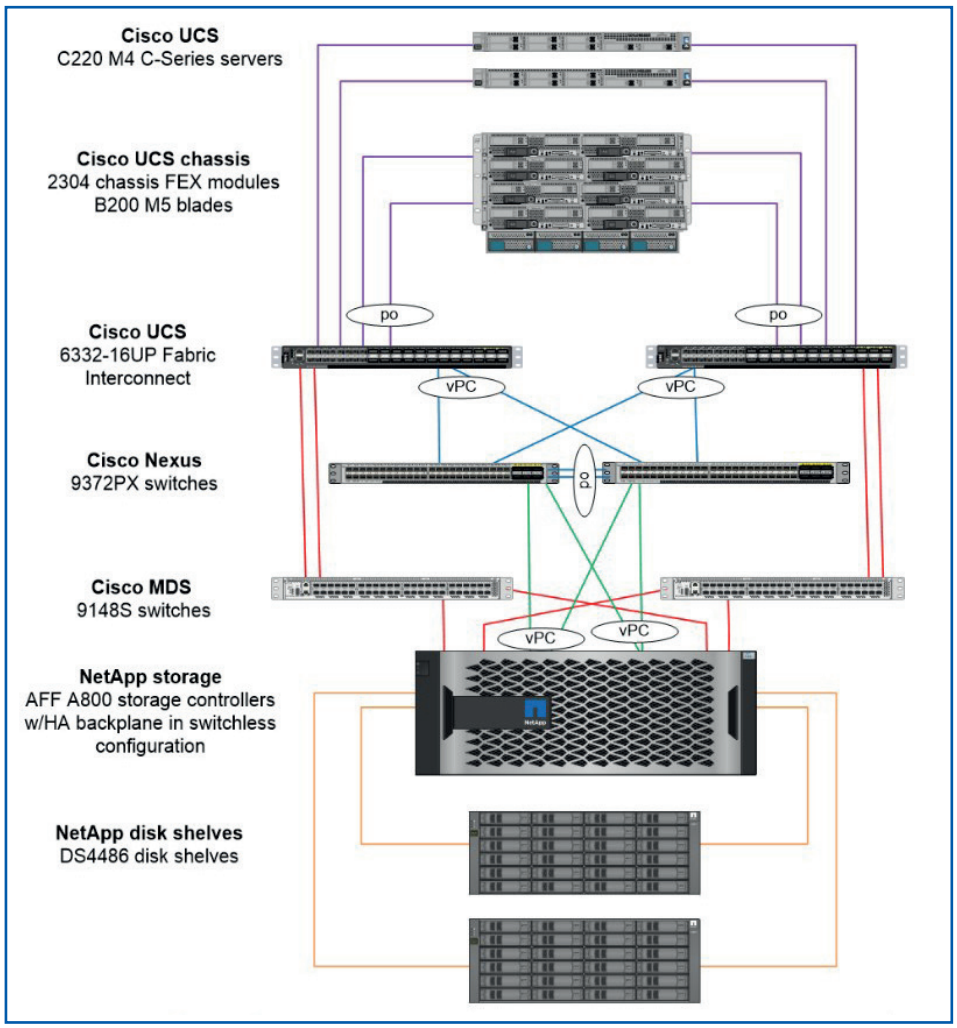

Abbildung 1: FlexPod Datacenter for Fibre Channel

Web Security aus der Cloud: Eine langfristige Option oder experimenteller Hype?

Fortsetzung von Seite 1

Timo Schmitz ist als Berater in den Bereichen IT-Sicherheit und Smart Technologies der ComConsult GmbH tätig. Im Projektgeschäft befasst er sich insbesondere mit den Themenbereichen Smart Environments sowie Cloud Security, von der konzeptionellen Phase bis hin zu einer praxistauglichen Umsetzung.

Frei nach dem Motto „Vertrauen ist gut, Kontrolle ist besser“ schützen sich Unternehmen neben der reinen Mitarbeitersensibilisierung selbstredend auch in technischer Hinsicht vor dem größten Angriffsvektor auf sensible Daten und die interne Infrastruktur: dem Internet. Hierzu bietet der Markt eine große Vielfalt verschiedener Lösungen an, die sich über unterschiedliche Appliances wie Secure Web/Mail Gateways bis hin zu ausgewachsenen Next Generation Firewalls mit zustandsorientierter Paketinspektion erstrecken. Die Absicherung des gen Internet gerichteten Verkehrs gewinnt zusätzlich zunehmend Bedeutung durch die Verlagerung von lokal installierter Software hin zu „Cloud-based Applications“ bzw. Software-as-a-Service-Produkten, deren Datenhaltung und Verarbeitung ins Internet, sprich: die Cloud, ausgelagert wird. Einige Sicherheitsunternehmen nahmen diesen Trend zum Anlass, um ihre Sicherheitslösungen ebenfalls teilweise oder komplett in die Cloud zu verlagern und dadurch Abstand von der klassischen Hub-and-Spoke Topologie zu nehmen (siehe Abbildung 1).

Ein weiterer Grund ist der in den vergangenen Jahren stark fortgeschrittene Wandel des Arbeitsalltags von Unternehmensmitarbeitern: Ein Unternehmen kann nicht mehr davon ausgehen, dass Zugriffe seiner Mitarbeiter auf das Internet ausschließlich aus dem internen Firmennetzwerk erfolgen. Mitarbeiter sind deutlich mobiler unterwegs und arbeiten häufiger im Sinne eines „Road -Warriors“ aus dem Home-Office oder unterwegs. Zusätzlich nutzen sie mobile Geräte wie Smartphone oder Tablets, um mit Unternehmensanwendungen zu arbeiten, die ggf. gar keinen direkten Zugriff auf das Firmennetz erfordern. Nichtsdestotrotz werden dort unter Umständen sensible Daten verarbeitet, und ein Unternehmen hat daher ein Eigeninteresse daran, auch solche Geräte bzw. Zugriffe abzusichern. Ein Perimeterschutz alleine ist also nicht mehr ausreichend.

Wir möchten in diesem Artikel das Phänomen „Web Security in der Cloud“ genauer beleuchten, um zu prüfen, ob Unternehmen einen echten Vorteil daraus ziehen können oder ob es sich dabei womöglich nur um einen Trend handelt, der sich auf langfristige Sicht ggf. als das falsche Zugpferd herausstellen könnte.

Sehen wir uns den aktuellen Markt genauer an, erkennen wir, welchen disruptiven Effekt Cloud-basierte Web-Security-Lösungen erzeugen, siehe Abbildung 2. Der Großteil der im Gartner Report über Secure Web Gateways [1] genannten Unternehmen bietet „konventionelle“ On-Premises Secure Web Gateways an. Darunter mischen sich jedoch auch Hybrid-Lösun-

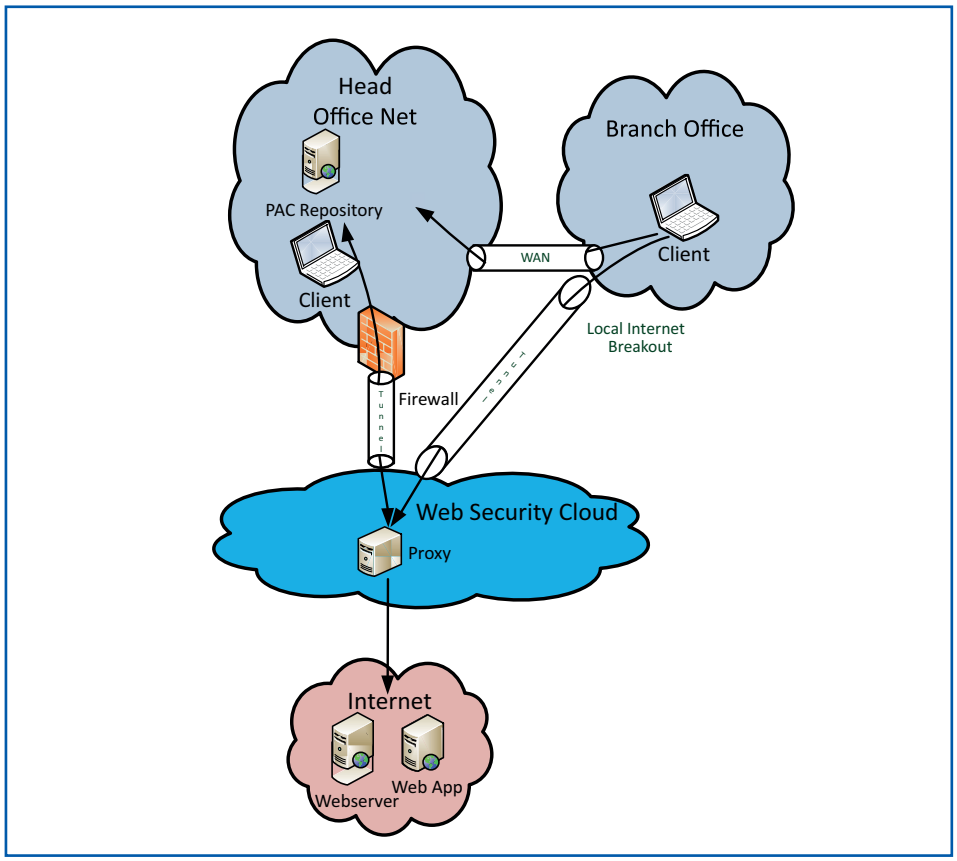

Abbildung 1: Simplifizierte Netzwerktopologie einer Web-Sicherheitslösung in der Cloud

Web Security aus der Cloud: Eine langfristige Option oder experimenteller Hype?

Abbildung 2: Gartner Magic Quadrant "Secure Web Gateways" 2018 [1]

gen (bspw. Symantec) sowie Unternehmen, die nahezu ausschließlich Cloud-basierte Lösungen anbieten (bspw. Zscaler). Diese „Cloud-only"-Lösungen mischen den Markt stark auf: So wurde Zscaler bspw. im Gartner Report von 2018 zum 8. Mal in Folge als „Leader" im Segment der Secure Web Gateways benannt.

Der Status Quo

Gehen wir einen Schritt zurück und blicken auf das Gefahrenpotenzial und den Zustand der gegenwärtigen Internetnutzung, um Anforderungen an die Sicherheit identifizieren zu können: Vergangenes Jahr entschloss sich Google dazu, auf die besondere Kennzeichnung von TLS-verschlüsselten Webseiten zu verzichten, da „Nutzer erwarten sollen, dass das Web standardmäßig sicher ist" [2]. Die Statistiken geben Google zumindest in der Hinsicht Recht, dass der absolute Löwenanteil der Webseiten, welche ein Nutzer täglich aufruft, über TLS verschlüsselt sind: Gemäß Google Transparency Report [3] waren beispielsweise 90 % der Webseiten, die deutsche Chrome-Nutzer am 17. August 2019 aufriefen, via TLS verschlüsselt, siehe Abbildung 3.

Die Aussage von Google bezogen auf die Sicherheit des Internets als solches ist jedoch mit Vorsicht zu genießen: Dass eine Webseite ausschließlich über einen verschlüsselten Kanal Inhalte vermittelt, ist grundsätzlich zwar die richtige Richtung hin zu einem Internet, welches ein größeres Augenmerk auf den Datenschutz und die Privatsphäre des Nutzers legt. Jedoch bedeutet dies nicht, dass die publizierten Inhalte per se keinen Schadcode enthalten können. Bei wenig technikversierten Nutzern erzeugt die zitierte Maxime den Eindruck, dass eine Seite grundsätzlich vertrauenswürdig ist, wenn ihr Browser sie als „sicher" kennzeichnet. Das ist aber keineswegs der Fall: Laut Auswertungen des Herstellers Zscaler verbirgt sich über 50% der Malware mittlerweile hinter SSL-/TLS-Verschlüsselung (siehe [4]). Zudem steige die Verbreitung der Malware über diesen Kanal rasant an (30% mehr Malware in einem Zeitraum von 6 Monaten, siehe [5]).

Dieser Zustand ist jedoch logisch bedingt durch die Weiterentwicklung des Mediums „Internet": Nutzer werden sensibilisiert und angehalten, sich von nicht vertrauenswürdigen Webseiten (sprich: regulären HTTP-Seiten) fernzuhalten. Also entwickeln Angreifer Methoden, um ihren Schadcode über vermeintlich vertrauenswürdige Wege zu verbreiten. Der Aufwand ist bspw. dank „Domain-validierten Zertifikaten" und kostenfreier Zertifizierung (bspw. durch Anbieter wie „Let's Encrypt") nicht sonderlich groß.

Ein verschlüsselter Kanal bewirkt, dass die Kommunikation zwischen Client und Server nicht abgehört, aber auch nicht auf Schadcode inspiziert werden kann. Unternehmen haben selbstverständlich dennoch ein großes Interesse daran, diesen Angriffsvektor abzusichern. An dieser Stelle kommt die Technik der „SSL/TLS Inspection/Interception" ins Spiel: Vor der Etablierung der TLS-Session mittels HTTP CONNECT Header öffnet das Secure Web Gateway bzw. der Proxy das Paket, um als „friendly Man-in-the-Middle" zu agieren und dies auch gegenüber dem Client zu kommunizieren (Einsatz eines vertrauenswürdigen Zertifikats).

Wir schließen aus den obigen Aussagen zum verschlüsselten Verkehr, dass ein erheblicher Sicherheitsgewinn auf dem Transportweg aus dem Einsatz von TLS/SSL Inspection geschöpft werden kann. Für TLS in den Versionen 1.0 – 1.2 trifft diese Aussage auch vollkommen zu,

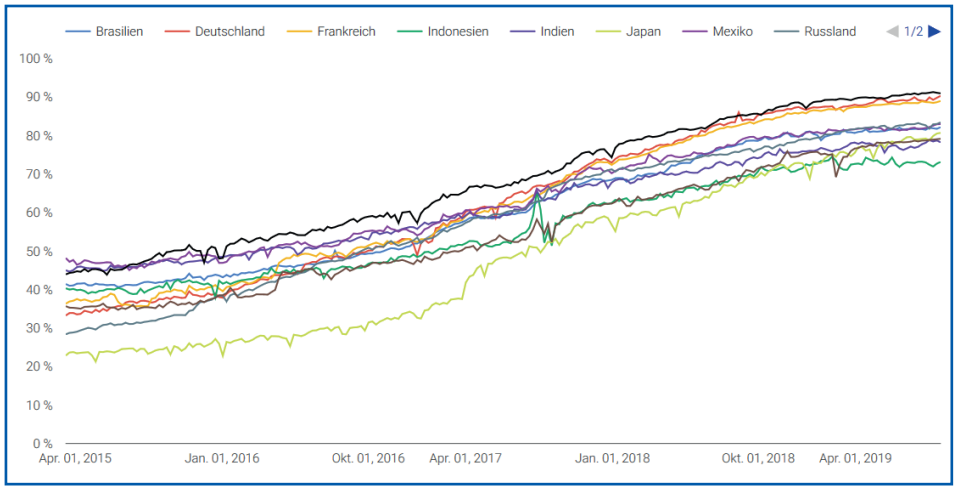

Abbildung 3: Prozentsatz der in Chrome über HTTPS geladenen Seiten nach Land [3]