März 2022

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Strategische IT-Planung - Heute schon tun, woran andere erst morgen denken

von Tanja Ulmen

Viel zu oft ist IT-Planung ein eher reaktiver Prozess. Vielleicht sind die Ambitionen zur strategischen IT-Planung am Anfang noch groß, doch diese vergehen oftmals schnell. Welche Gedanken sollte man sich daher machen, um IT nachhaltig und strategisch zu planen? Wie kann man Ziele schon im Voraus so formulieren, sodass sie einhaltbar werden? Welche Schritte sollten berücksichtigt werden, und aus welchen Maßnahmen bestehen die einzelnen Schritte?

Seite 6

Wird RZ-Mikrosegmentierung Best Practice?

von Dr. Behrooz Moayeri

Bereits vor fast drei Jahren hat mein Kollege Dr. Hoff im Netzwerk Insider die Notwendigkeit der Mikrosegmentierung in modernen Zonenkonzepten festgestellt.

Seite 2

MultiCloud-Anbindung – Herausforderungen und Lösungsansätze

von Martin Egerter

Nachdem die ersten Cloud-Angebote etwa Mitte der 2000er Jahre am Markt erschienen sind, waren viele Unternehmen gegenüber diesen Angeboten trotz der gepriesenen Vorteile, die zwischenzeitlich in einer Vielzahl von Fachartikeln, Blog-Beiträgen, etc. dokumentiert sind, zunächst skeptisch eingestellt.

Seite 20

Webinar der Woche

Voice over LTE und der Weg nach 5G

Seite 18

Der Umgang mit Sicherheitsforschern – ein Thema für sich

von Dr. Markus Ermes

Immer wieder hört man von Sicherheitsforschern, die Entwickler oder Firmen über Sicherheitslücken in ihren Produkten aufmerksam machen. Die Reaktion der Unternehmen und Entwickler fällt dabei sehr unterschiedlich aus. Schauen wir uns ein paar typische Reaktionen an.

Seite 17

Wird RZ-Mikrosegmentierung Best Practice?

von Dr. Behrooz Moayeri

Fortsetzung von Seite 1

Im selben Jahr, 2019, ist unser Kollege Dr. Ermes auf Mikrosegmentierung mit VMware NSX eingegangen. Vor zwei Jahren habe ich selbst auf die Möglichkeit der Mikrosegmentierung als Erfolgsfaktor von großen Clouds hingewiesen. Im Vergleich zu diesen großen Clouds haben OnPrem-Rechenzentren immer noch einen großen Nachholbedarf, was Mikrosegmentierung betrifft. Nun mehren sich Anzeichen, dass eine zunehmende Anzahl von Herstellern hierzu Lösungen anbietet.

Warum Mikrosegmentierung?

Angriffe auf IT-Infrastrukturen nehmen zu. Wir haben längst hingenommen, dass in IT-Infrastrukturen eingesetzte Software Angriffsflächen bietet. Wir werden kaum mehr überrascht, wenn eine neue Sicherheitslücke oder gar ein gravierender Angriff unter Nutzung einer neuen, bisher unbekannten Sicherheitslücke bekannt wird.

Wenn Software per se angreifbar ist, muss es umso mehr darauf ankommen, erstens die Exponiertheit von Systemen auf das erforderliche Minimum zu reduzieren und zweitens das Ausmaß der durch kompromittierte Software und Hosts entstehenden Schäden zu minimieren.

Beiden Zielen dient die Mikrosegmentierung. Mit ihr wird die Kommunikation eines Hosts auf das notwendige Minimum herabgesetzt. Das System ist dann weniger exponiert. Außerdem sorgt Mikrosegmentierung dafür, dass der Angreifer, der einen Host kompromittiert hat, weniger Möglichkeiten lateraler Fortbewegung vorfindet. Der kompromittierte Host kann bei Anwendung von Mikrosegmentierung nicht in dem Maße als Sprungbrett für weitere Angriffe missbraucht werden wie es in einem flachen Netz möglich ist.

Probleme bei der Mikrosegmentierung

Die Virtualisierung erschwert die Mikrosegmentierung. Zwei virtuelle Maschinen auf demselben Host können über den virtuellen Switch im Hypervisor miteinander kommunizieren, ohne das physische Netz außerhalb des Hosts nutzen zu müssen.
Deshalb muss die Mikrosegmentierung auch die Einschränkung der Kommunikation über den virtuellen Hypervisor-Switch umfassen. Der Lösungsanbieter für die Virtualisierung ist in der Lage, dafür zu sorgen. Mit VMware NSX wird genau das erreicht. NSX beinhaltet eine verteilte Firewall-Funktion, die trotzdem zentral verwaltet wird. Firewall-Regeln werden zentral definiert und lokal auf allen Hosts durchgesetzt. Das ist in einer Umgebung, in der sowohl die zentrale Verwaltung der Hosts und der VMs als auch der virtuelle Hypervisor-Switch vom selben Hersteller stammen, nicht sehr schwer.

Schwieriger wird es, wenn die Mikrosegmentierung nicht nur in der VMware-vSphere-Umgebung, sondern auch für andere Systeme, sei es für physische Server oder für andere Hypervisor, zentral gesteuert werden muss.

Cisco ACI

Hier hatte Cisco mit Application Centric Infrastructure (ACI) jahrelang einen Vorsprung vor anderen Herstellern. Mit ACI können End Point Groups (EPGs) definiert werden, deren Kommunikation zentral reglementiert werden kann. EPGs können sowohl physische als auch virtuelle Server umfassen.

Um die Kommunikation über Hypervisor-Switches einzuschränken, bedient sich Cisco ACI eines einfachen Mittels: Auf den virtuellen Hypervisor-Switches wird die längst als Standardfunktion genutzte Methode Private Virtual Local Area Network (PVLAN) genutzt. Die gesamte Kommunikation der VMs wird dabei über den physischen Switch außerhalb des Hosts geführt. Dieser kann die Kommunikation einschränken. Dafür muss es eine Schnittstelle zwischen den Management-Werkzeugen von VMware vSphere und Cisco ACI geben. Cisco nutzt dazu offengelegte Application Programming Interfaces (APIs) auf VMware-Seite.

HPE Aruba zieht nach

Der PVLAN-Trick wird nun auch von HPE Aruba angewandt. Der Hersteller bietet mit dem Produkt CX 10000 einen Switch an, der auf der Zusammenarbeit mit Pensando basiert. Pensando hat sich auf die Fahne geschrieben, „die Cloud bis zum Edge zu erweitern“. Das ist so zu verstehen, dass Komponenten am Rande des Netzes, d.h. möglichst nah an den Endsystemen, die Intelligenz bieten, die wir von Clouds kennen. Das wird mit einem programmierbaren Prozessor erreicht, der in Server und Switches eingebaut wird und Funktionen wie Stateful Inspection übernehmen kann.

Die Pensando Distributed Services Card (DSC) ist mit einem solchen Prozessor ausgestattet. Die DSC kann als Network Interface Card (NIC) in HPE-Servern zum Einsatz kommen.

Strategische IT-Planung - Heute schon tun, woran andere erst morgen denken?

von Tanja Ulmen

Fortsetzung von Seite 1

Das und weitere Hintergründe möchte ich in diesem Artikel gerne erläutern und darauf eingehen, was man *heute schon tun kann, woran andere erst morgen denken?*

Dieses Zitat wird Heraklit von Ephesos zugeschrieben, einem griechischen Philosophen (ca. 550-480 v. Chr.). Seine Worte bezogen sich auf jegliche Vorhaben und sind sehr gut auf strategische IT-Planung anwendbar. Letztere bedeutet vorausschauendes Entscheiden und stellt damit eine nicht zu unterschätzende Herausforderung dar.

Warum strategisch?

Zunächst einmal, was spricht gegen einen reaktiven Prozess? Prozesse, Projekte, Changes etc., die reaktiv geplant werden, zeichnen sich oftmals durch wenig Weitsicht aus. Hier kann es schon mal dazu kommen, dass eine Budget-Planung hinten und vorne nicht reicht, Mitarbeiter überlastet und genervt sind, immer wieder Situationen eintreten, die überfordern und Hau-Ruck-Entscheidungen erzwingen, und vor allem hinten raus wenig Mehrwert entsteht. Da das Ganze natürlich kaum dokumentiert wird, findet man sich in solchen Situationen immer und immer wieder. Sprich, es endet oft im Chaos.

Definition

Um mal einen Schritt zurückzugehen: Was bedeutet strategische IT-Planung genau? Leider ist schon der Begriff Strategie schwierig zu definieren. Laut Duden ist Strategie ein „genauer Plan des eigenen Vorgehens, der dazu dient, ein militärisches, politisches, psychologisches, wirtschaftliches o. ä. Ziel zu erreichen, und in dem man diejenigen Faktoren, die in die eigene Aktion hineinspielen könnten, von vornherein einzukalkulieren versucht“.

Bei Wikipedia findet man direkt mehrere Seiten: Strategie (Militär), Strategie (Schach), Strategie (Spieltheorie), Strategie (Wirtschaft). Gemeinsam haben sie den Punkt, dass eine Strategie dazu dient, einen Plan zu entwickeln, um langfristige Ziele zu erreichen.

Der wichtige Teil steckt meiner Meinung nach in der Duden-Definition, und zwar in der Erwähnung der Risiken, bzw. *Faktoren, die in die eigene Aktion hineinspielen könnten*. Diese müssen entgegen einer, wie ich glaube, weitläufigen Meinung nicht zwangsläufig vermieden, sondern stattdessen eingeplant werden. Unvorhergesehenes lässt sich schwer vermeiden, doch wenn man weiß, was man tut und warum man etwas tut, kann man definitiv besser mit Unerwartetem umgehen, und genau darum geht es.

Jetzt zurück zur strategischen IT-Planung – was bedeutet es also, wenn ich IT-Planung strategisch angehe? Vielleicht kann man sich hier mit vorhandenen Standards oder Richtlinien weiterhelfen. Bei ITIL 4 beispielsweise spricht man oft von einer ganzheitlichen Planung, was dem schon sehr nahekommt.

ITIL – für die, die es nicht kennen – ist eine Sammlung von Best Practices zur Bereitstellung von IT-Services. In den ITIL-Büchern

Geflutete IT-Technik - Schadensaufnahme und Handlungsempfehlungen

Mit Thomas Lothar sprach Christiane Zweipfennig

Der Sommer 2021 war geprägt von starken Regenfällen. Mitte Juli wurden unter anderem in Nordrhein-Westfalen aus kleinen Flüssen und Bächen reißende Ströme, die ganze Ortschaften und die Existenz von vielen Menschen zerstörten.

Vielerorts waren auch öffentliche Einrichtungen betroffen. Thomas Lothar, Senior-Berater mit langjähriger Erfahrung in der Installation von lokalen Netzen bei ComConsult, war nach der Flutkatastrophe vor Ort.

Du bist eines der Urgesteine von ComConsult. Wie lange bist du schon im Unternehmen und was sind deine Beschäftigungsfelder?

Ich hatte Anfang des Jahres dreißigjähriges Jubiläum, ich gehöre also quasi zum Inventar (lacht). Zu Beginn habe ich die Abteilung Netzwerkdokumentation mit aufgebaut. Dann bin ich in den Planungsbereich gewechselt. Dort befasse ich mich mit der Planung von Datennetzen und Rechenzentren sowie dem Betrieb von Netzwerken.

30 Jahre bei ComConsult. Da kommen jede Menge Projekte zusammen.

Ja. Wir haben beispielsweise für ein großes Logistikunternehmen den Neubau der Zentrale geplant und über zehn Jahre mit bis zu acht Kollegen den kompletten Netzwerkbetrieb für die alte Zentrale und fünfzehn Außenlokationen erbracht. Danach war Frankfurt nahezu meine zweite Heimat, wo ich fast zwölf Jahre das Netzwerk für den Neubau und zwei weitere Hochhäuser einer Bank mit geplant und umgesetzt habe. Das Rechenzentrum hat eine Fläche von 1.500 Quadratmetern und wir haben nur in dem Neubau zwei Millionen Meter Kupferdatenkabel verlegt und 35.000 Endgeräteanschlüsse realisiert.

Im Moment planen wir für das Rechenzentrum eines mittelständischen Produktionsunternehmens eine ausfallsichere Stromversorgung. In diesem Unternehmen, das europaweit tätig ist, war die Stromversorgung in einem Serverraum ausgefallen und das hatte Auswirkungen auf alle Standorte.

Als Mitte Juli bei uns im Aachener Raum das Wasser über die Ufer stieg, wurde ComConsult in Kooperation mit Drees & Sommer damit beauftragt, mehrere öffentliche Einrichtungen im Stadtgebiet Eschweiler zu begehen und den entstandenen Schaden zu begutachten. Wie war die Situation vor Ort?

Wir waren an der Schadenserhebung von sieben Gebäuden beteiligt. Bei einigen hatte das Erdgeschoss kurze Zeit bis zu vierzig Zentimeter und das Untergeschoss tagelang komplett unter Wasser gestanden. Wir wurden zwei Wochen nach der Katastrophe zur Schadensaufnahme gerufen. Da war das Wasser schon abgepumpt worden, die Aufräumarbeiten im Gange, viele Räume schon leer und draußen vor den Gebäuden lagen riesige Müllhalden mit nicht mehr brauchbaren Möbeln, Isolierungen, aufgeweichten Ordnern und so weiter.

MultiCloud-Anbindung – Herausforderungen und Lösungsansätze

von Martin Egerter

Fortsetzung von Seite 1

Zu Beginn des „Cloud-Zeitalters“ existierten neben der allgemeinen und grundsätzlichen Skepsis oftmals auch Bedenken hinsichtlich des Datenschutzes und/oder der technischen Hürden, die es zu überwinden galt.

Doch in der Zwischenzeit hat sich das deutlich verändert, sodass nicht nur junge und moderne Start-Up-Unternehmen, sondern zunehmend auch Unternehmen aus allen Branchen derartige Angebote nutzen, oder zumindest deren Einführung in Erwägung ziehen.

Nach Erfahrungen des Projektgeschäftes von ComConsult ist mittlerweile nicht nur der Einsatz von Cloud-Lösungen klar und deutlich erkennbar. Es ist darüber hinaus eindeutig festzustellen, dass ein Cloud-Anbieter in der Regel nicht alle Anforderungen erfüllen kann. Insofern wundert es nicht, dass Unternehmen in zunehmendem Maße mehrere und unterschiedliche Cloud-Angebote nutzen, um die jeweiligen Workloads optimal zu verteilen.

Dieser deutlich erkennbare Trend wirft gleichzeitig automatisch Fragen hinsichtlich der Anbindung und der Integration mehrerer Cloud-Provider auf.

Der vorliegende Artikel greift diese Fragen auf und skizziert mögliche Lösungsansätze, mit denen man den Herausforderungen, die sich automatisch aus der gleichzeitigen Nutzung mehrerer Clouds ergeben, begegnen kann.

Die schlechte Nachricht vorab - und das sei schon vorweggenommen: Es gibt keine „One-Size-Fits-All“-Lösung - in diesem Kontext könnte man auch sagen „One Cloud Fits All“ - zumal sich in der Regel die Ausgangsvoraussetzungen individuell und je nach Anwendungsfall unterscheiden. Doch auch wachsende Sicherheitsbedenken und strengere Compliance-Vorschriften beeinflussen die zunehmende Nutzung von Hybrid- und Multi-Cloud-Lösungen. Anstatt alle Daten und Anwendungen in die Public Cloud zu migrieren, ziehen es einige Unternehmen deshalb vor (oder sind sogar verpflichtet), einige Daten OnPrem in der eigenen Umgebung zu halten, um das Risiko von Verstößen gegen Sicherheits- und Compliance-Anforderungen zu verringern oder einfach nur, um konkrete Kundenanforderungen zu erfüllen.

Andere wiederum versprechen sich zusätzlich, das Risiko eines „Vendor-Lock-Ins“ zu minimieren, Kosten zu reduzieren und es zu vereinfachen, innovativ und flexibel zu bleiben, indem sie nur die besten Funktionen jedes Cloud-Anbieters nutzen.

Doch trotz all dieser Vorteile kann die Einrichtung und Nutzung mehrerer Umgebungen die Komplexität insgesamt erhöhen und zu neuen Problemen im täglichen Betrieb und dem Management führen.

Wir wollen zunächst den Unterschied zwischen dem Hybrid- und dem Multi-Cloud-Modell herausarbeiten: