ComConsult Research

Der Netzwerk Insider

April 2014

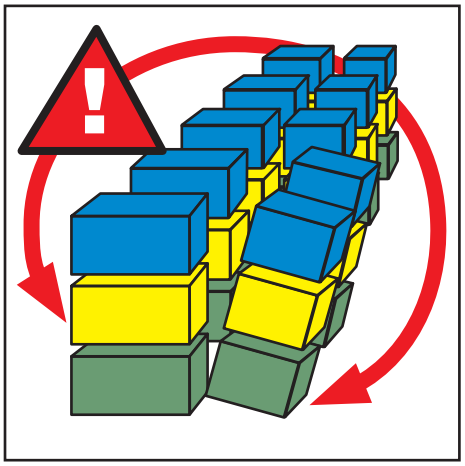
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Data Center in a Box und die Folgen für die Informationssicherheit

von Dr. Simon Hoff, Dipl.-Inform. Sebastian Jansen, Dr. Melanie Winkler

Ein neuer Trend hat das moderne RZ erfasst: Lösungen für Data Center in a Box etablieren sich immer sichtbarer als neues Konzept. Die Hersteller versprechen integrierte Systeme, die eine RZ-Automatisierung erst richtig möglich machen. Nun hat Integration nicht nur Vorteile. Je dichter Systeme zusammenrücken, desto stärker sind die Abhängigkeiten voneinander und dies führt automatisch zur Frage, ob hierdurch neue Risiken für die Informationssicherheit entstehen und neue Sicherheitsmaßnahmen erforderlich werden. Dieser Artikel analysiert mit FlexPod, Vblock und PureSystems einige Vertreter des Data Center in a Box und stellt ein übergreifendes Maßnahmenbündel zur Absicherung solcher Lösungen vor.



1. Grenzenlose Virtualisierung und Automatisierung in modernen RZ-Architekturen

Typisch für RZs ist ein mehrstufiger Aufbau, der die Ebenen Netzwerk, Compute (d.h. Server) und Storage umfasst. In der Vergangenheit wurde das RZ-Design typischerweise in einem Best-of-Breed-Ansatz auf jeder Ebene unabhängig von anderen Ebenen (z.B. hinsichtlich Leistung und Funktionalität) vorgenommen.

weiter auf Seite 6

Zweitthema

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 3

von Dipl.-Inform. Petra Borowka-Gatzweiler

7. Einbindung virtueller Netzkomponenten

Im Rahmen der Evolution von Virtualisierung lassen sich aktuell auf Hostsystemen nicht nur virtuelle Switches (vSwitches, vSw) sondern auch virtuelle Router (vRouter, vR), virtuelle Load Balancer (vLB) oder virtuelle Firewalls (vFW) installieren. Sichtbar werden solche Switches über Management-Anpassungen bzw. Zusatzmodule der Netzwerk-Hersteller für die etablierten Virtualisierungs-Umgebungen, hauptsächlich VMware und Hypervisor.

Nach außen sichtbar und mit Anschluss an einen physischen Netzwerk-Switch sind nur die physischen NICs (phyNIC). Diesen werden gegebenenfalls – oder auch nicht – Ports der vSwitches zugeordnet, über die sie nach draußen kommunizieren können. Auf die host-interne Kommunikationsfähigkeit hat der physische Netzwerk-Access Switch im Regelfall keine Einflussmöglichkeit. Der vSwitch kann ähnlich wie ein physikalischer Switch konfiguriert sein und nach innen über vNICs die VMs anbinden, nach außen über zugeordnete phyNICs mit anderen Systemen kommunizieren.

weiter Seite 20

Geleit

QoS: wieder auf der Tagesordnung?

auf Seite 2

Oster-Spezial

Sonderaktion Video-Abo im April bei ComConsult-Study.tv

auf Seite 18

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2014

ab Seite 4

Neues Seminar

Tod des Tischtelefons und danach Cloud-Lösungen?

auf Seite 19

Zum Geleit

QoS: wieder auf der Tagesordnung?

Quality of Service QoS war ein intensives Diskussionsthema speziell in den 90er Jahren als die Bandbreiten in Netzwerken zusammen mit dem realen Bedarf schnell von 10 Mbit auf Gigabit gewachsen sind. Dabei ist die Kombination sehr unterschiedlicher Bandbreiten in Netzwerken immer ein Indikator für mögliche Engpass-Bereiche. Mit dem Übergang auf Gigabit-Netzwerke hat sich QoS von einem realen Bedarfsthema zu einem SLA-Feigenblattthema gewandelt. Speziell für Voice und Video in Netzwerken wurde von einigen Herstellern pauschal die Notwendigkeit von QoS unterstellt. Dies wurde unterstrichen mit zum Teil abenteuerlichen Labor-Vorführungen, die die Auswirkungen eines blockierten Netzwerkes auf Sprachübertragungen belegten.

In der Praxis konnte ein wirklicher Bedarf für QoS in Gigabit-Netzwerken kaum nachgewiesen werden (bis auf begründete Ausnahmen). So wurde es mehr als Vorsichtsmaßnahme und zur Fehlerabgrenzung eingesetzt.

Nun stehen wir im Moment mitten im Übergang auf 10, 40 und 100 Gigabit-Netzwerke. Damit sollte das Thema ja nun doch endgültig in der Mottenkiste der LANs verschwinden, oder?

Tatsächlich aber hat sich die Lage in den letzten Jahren deutlich verkompliziert. Die Ursache liegt in mehreren Faktoren begründet:

- Die Trennung von Server und Speicher im Rechenzentrum kann zu erheblichen Datenströmen im Netzwerk zwischen Server und SAN oder NAS führen

- Virtualisierungs-Lösungen können je nach Auslegung zum Beispiel im Bereich High-Availability hohe Anforderungen an Netzwerke stellen und zu star-

ken Spitzenlasten führen

- Wir sind wieder in einer Situation, in der sehr unterschiedliche Bandbreiten zusammen kommen. 1, 10, 40 und 100 Gigabit spannen ein erhebliches Bandbreiten-Spektrum auf.

Wie schon früher liegt auch heute ein Problem in möglichen Engpässen durch Überbuchungen von Switch-Systemen. Bei Datenströmen im 10 Gigabit-Bereich sind auch größere Puffer schnell gefüllt. Außerdem sind Puffer ein Preisfaktor für die Hersteller und Einsparungen an dieser Stelle können sich schnell negativ auswirken.

Der Übergang zu 1, 10, 40 und 100 Gigabit-Netzwerken führt also zu einer Wiederbelebung des QoS-Themas.

Also alles wie gehabt, packen wir die VLANs aus und sichern unsere kritischen Datenströme mit Prioritäten ab?

Dies ist Mitnichten der Fall und die Realität ist deutlich komplexer:

- Prioritäten sind wenn überhaupt ein Mechanismus, um kleine Datenströme vor großen zu schützen. Damit also zum Beispiel Sprach-Verbindungen auch in stark belasteten Netzwerken funktionieren

- Unsere neue Betriebssituation wird aber durch extrem große Datenströme bestimmt, die auch selber eine hohe Priorität bräuchten

Um dem gerecht zu werden, hat man speziell neue Verfahren wie DCB geschaffen, die eben genau dieser Situation Rechnung tragen. Gleichzeitig wird es immer schwerer ein traditionelles VLAN-Design umzusetzen. Der VLAN-Mechanismus wird der modernen Netzwerk-Situation nicht mehr gerecht.

Wir brauchen also eine neue QoS-Diskussion, die sich mit den Fragen befasst:

- Wo bestehen QoS-Risken bzw. Bedarfssituationen?

- Welche QoS-Verfahren machen Sinn?

- Wie sieht eine angemessene LAN-Planung aus, die diese Probleme verhindert?

- Was passiert an der Grenze zum WAN, an der immer größere LAN-Datenströme auf die Beschränkungen im WAN stoßen?

Wir greifen diese Diskussion mit einer Sonderveranstaltung auf. Versäumen Sie nicht, sich einen Platz zu diesem hoch aktuellen Thema zu sichern.

Ihr
Dr. Jürgen Suppan

Sonderveranstaltung

Quality of Service - Sonderveranstaltung
30.10.14 in Bonn

Die Devise lautete bislang „Wer im LAN QoS braucht, hat Probleme, die sich mit QoS nicht wirklich lösen lassen“.
Veränderte Datenströme erfordern aber moderne Designs und neue Technologien und Protokolle bieten verbesserte Ansätze.
Wo steht QoS heute? Die Sonderveranstaltung erläutert, wo QoS heute steht.

Referenten u.a.: Dipl.-Inform. Petra Borowka-Gatzweiler, Dipl.-Math. Cornelius Höchel-Winter, Dr. Behrooz Moayeri
Preis: € 990,-- netto

Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2014

15.05. - 16.05.14 in Bonn

Die ComConsult Akademie veranstaltet vom 15.05. bis 16.05.14 ihr "ComConsult IT-Sicherheits-Forum 2014" in Bonn.

Folgende Themenbereiche werden behandelt:

- Für den Nutzer einer virtuellen IT im Zeitalter des Cloud Computing muss sich die Informationssicherheit auf ihren Namen besinnen und Sicherheitsmaßnahmen müssen sich auf die Informationen selbst konzentrieren. Kernelemente sind nicht nur die Zusicherung von Vertraulichkeit und Authentizität durch Verschlüsselungstechniken sondern immer mehr auch die Nachvollziehbarkeit von Änderungen an Daten (Revisionsfähigkeit) und die Kontrolle von unerwünschtem Abfluss von Daten, d.h. letztendlich Klassifikation von Daten in Verbindung mit Data Loss Prevention.

- Die Absicherung von UCC muss verstärkt den Aspekt der Zusammenarbeit unterschiedlicher Unternehmen und Behörden berücksichtigen. Hier sind nicht nur Maßnahmen zur Absicherung von

Voice und Video gefragt. Sicherheitsmaßnahmen müssen alle Kom-munikationskanäle in UCC berücksichtigen, vom Chat, über Anwendungs- und Desktop-Sharing bis zum flexiblen Dokumentenaustausch.

- Wenn unterschiedliche, heterogene Gruppen von Nutzern und Geräten auf unterschiedlichem Sicherheitsniveau eine gemeinsame IT-Infrastruktur nutzen, muss diese in einem gewissen Umfang mandantenfähig sein. Dies erfordert stets die sichere Trennung der Informationen der Mandanten.

- Die traditionelle Methode der Informationssicherheit einer möglichst physikalischen Trennung auf Ebene des Netzes und der Endgeräte ist nicht mehr zeitgemäß. Virtuali-sierung erfordert ein Umdenken in Richtung logischer Trennung und insbesondere in Richtung kryptographischer Techniken.

- Zonenkonzepte in RZ und Campus sind zu einem normalen Gestaltungsinstrument geworden, stellen aber durch ihre Komplexität höchste Ansprüche an Planung und Betrieb. Schwerpunkte sind dabei die logische Trennung von Zonen in Virtualisierungsplattform, Netz und im Storage-Bereich.

- Wir benötigen sichere Identitäten in IP-Netzen und auf dieser Basis eine Netzzugangskontrolle mit dynamischer Berechtigung von Zugriffen

Fax-Anmeldung 02408/955-399 oder 02408/955-398

Hiermit melde ich mich verbindlich zum **ComConsult IT-Sicherheits-Forum 2014** an.

☐ **Kongress**

vom 15.05. bis 16.05.14 in Bonn zum Preis von € 1.990,-- netto

☐ **Bitte reservieren Sie für mich ein Zimmer**

vom _____ bis zum _____14
im Günnewig Hotel Bristol Bonn zum Sonderpreis von 112,-- € inkl. Frühstück

_____ Vorname,

_____ Nachname

_____ Firma

_____ Straße

_____ PLZ, Ort

_____ Telefon, Fax

Ich habe die Kongressbedingungen zur Kenntnis genommen.

_____ E-Mail

_____ Datum, Unterschrift

Programmübersicht - ComConsult IT-Sicherheits-Forum 2014

Donnerstag 15.05.2014

9:30 Uhr (45 Minuten)
Keynote: Grenzenlose Mobilität und Virtualisierung in der IT: Stürmische Zeiten für die Informationssicherheit
- Alles wird virtuell: Cloud Computing, Virtualisierung und Software-Defined Networking (SDN) veränderndie Informationssicherheit
- Overlay-Strukturen und Automatisierung im Rechenzentrum erfordern neue Sicherheitskonzepte
- Zonenarchitekturen: Warum wir neue Firewall-Konzepte brauchen
- Industrial Control Systems und autarke Systeme im Internet of Things: Potential für kritische Angriffe
- Sichere Integration mobiler Endgeräte: Mehr als Mobile Device Management
- Trennung dienstlicher und privater Daten auf mobilen Endgeräten: Auf die Plattform kommt es an

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:15 Uhr Kaffeepause

Themenblock: Sicherheit in Cloud und RZ

10:45 Uhr (30 Minuten)
Private Cloud und Zonenkonzepte in der Praxis
- Was ändert Private Cloud im Rechenzentrum? • Sind Private Cloud und traditionelle Zonenkonzepte vereinbar? • Automatisierung und Firewalling: ein Widerspruch?
- Welches Zonenkonzept passt zur Private Cloud? • Sicherheit von Overlay-Strukturen

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:15 Uhr (45 Minuten)
Data Center in a Box: Integrierte Referenzarchitekturen und Fertigklösungen im RZ
- Wie sehen moderne RZ-Architekturen aus? • Referenzarchitekturen und Fertiglösungen (vBlock, FlexPod, Pure Systems etc.) im Überblick • Welchen speziellen Gefährdungen sind solche Lösungen ausgesetzt? • Wie muss sich die IT-Sicherheit diesen Rahmenbedingungen anpassen?
- Sicherheitsmaßnahmen für integrierte RZ-Architekturen • Konzepte zur sicheren Mandantentrennung • Unter welchen Rahmenbedingungen können auch Systeme mit hohem Schutzbedarf auf solchen RZ-Lösungenbetrieben werden?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:00 Uhr Mittagspause

13:30 Uhr (45 Minuten)
Next Generation Firewall als Perimeter-Gateway in der Praxis
- Vom Portfilter zur Applikations-Awareness- von der IP-Adresse zur User-Identifikation: warum und wo man umdenken muss
- Einbindung unterschiedlicher Betriebssysteme und Geräte: Windows,OS X, iOS, Android
- Next Generation Firewall meets Next Generation Internet Protokoll oder IPv6 auf einer NGF: Was sofort klappt und wo es hakt • Fehler bei der Konfiguration, die man besser vermeidet

Markus Schaub, ComConsult Research Ltd.

14:15 Uhr (45 Minuten)
Virtuelle Sicherheitskomponenten
- Konsequenzen von Overlay-Netzen und RZ-Automatisierung für Firewalls
- Wie unterscheiden sich die heutigen Ansätze zur Firewall-Virtualisierung (Firewall-Kontexte, virtuelle Appliances, VM NIC Firewalls, ServiceInsertion in Software Defined Networks)?
- Für welche Szenarien ist welcher Firewall-Ansatz wie geeignet?
- Welche Leistungsfähigkeit ist von diesenLösungen zu erwarten?

Sebastian Jansen, ComConsult Beratung und Planung GmbH

15:00 Uhr Kaffeepause

15:30 Uhr (30 Minuten)
Cloud Computing und IT as a Service - Outsourcing in Zeiten grenzenloser Überwachung
- Begriffsbestimmung: Public Cloud, Private Cloud, Hybrid Cloud
- Cloud Computing als Konsequenz moderner Software- und IT-Architekturen
- Sicherer Umgang mit Anwendungen und Daten in Public Cloud, Hybrid Cloud und Private Cloud
- Beispiele Collaboration und MDM in der Cloud: Was ist aus Sicherheitsperspektive noch vertretbar?
- UCaaS - Attraktives Outsourcing-Modell oder Offenbarungseid? • UCaaS und Telefonie aus der Cloud - Gibt es einen Schutz vor Aufzeichnen von Verbindungsdaten und sogar Gesprächen? • Anforderungen an Cloud Provider Verankerung von Sicherheitsanforderungen in Verträgen und SLAs

Martin Egerter, ComConsult Beratung und Planung GmbH

Themenblock: Netzwerkevolution

16:00 Uhr (45 Minuten)
Nur eines ist sicher: Das Internet of Things kommt!
- Die Vision Internet of Things (IoT) • IoT ohne Ende: Vom Fahrzeug zum Lichtschalter
- IoT im produktionsnahen Umfeld: Industrie 4.0
- Risiken durch eine exponentielle Vermehrung der IPv4 und IPv6 Clients
- Sicherheitsaspekte bei einer dezentralen Intelligenz durch autonome Things

Dominik Franke, ComConsult Beratung und Planung GmbH

17:30 Uhr **Happy Hour**

Programmübersicht - ComConsult IT-Sicherheits-Forum 2014

Freitag 16.05.2014

9:00 Uhr
45 Minuten

Industrial Control Systems - zunehmende Sicherheitsproblematik und Gegenmaßnahmen
- Rolle von ICS im iOT
- Sicherheitsprobleme bei Automatisierungsanlagen
- Analyse eines Beispielsystems
- Vorgehensweise zum Schutz von ICS

Prof. Dr. Marko Schuba, Fachhochschule Aachen

9:45 Uhr
45 Minuten

Sichere Anbindung von externen UC-Partnern
- Trusted VoIP over Internet
- Private SIP Trunks als Allheilmittel?
- Federation & Presence: das Ende des Datenschutzes?
- Legacy Video: ein Sicherheitsrisiko?

Claus Elfering, ComConsult Beratung und Planung GmbH

10:30 Uhr Kaffeepause

Themenblock: Mobile und drahtlose Kommunikation

11:00 Uhr
45 Minuten

Enterprise Mobility: Schmelztiegel der Informationssicherheit
- Bedrohungen ohne Ende: Von der Lauschattacke bis zum Abfluss kritischer Daten
- Sandboxing, Virtualisierungstechniken und Verschlüsselung: Reichen solche Sicherheitsmechanismen aus?
- Profiling-Techniken, Erkennung von Endgeräten und Policy-Zuweisung
- Mobile Device Management und Company App Stores als Sicherheitsmaßnahmen: Möglichkeiten und Grenzen
- Sichere Netzanbindung und Abgrenzung unterschiedlicher Benutzergruppen
- Auswirkungen mobiler Endgeräte auf das RZ und seine Infrastrukturen

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

11:45 Uhr
45 Minuten

Malware-Analyse in Android:
Vorstellung gängiger Werkzeuge und Verfahren zur Untersuchung von Android-Malware
- Einführung in die Android-Systemarchitektur und Laufzeitumgebung
- Androids Rechtemodell und Application Sandboxing
- Statisches vs. dynamisches Reverse Engineering
- Einführung in verschiedene Tools anhand einer aktuellen Android Malware

René Werner, GAI NetConsult GmbH

12:30 Uhr Mittagspause

14:00 Uhr
45 Minuten

Trennung privater und dienstlicher Daten auf mobilen Endgeräten: Usability vs. Security
- BYOD oder private Nutzung mobiler Endgeräte: Anforderungen der Nutzer und der Informationssicherheit im Widerspruch
- Container-Techniken und Virtualisierung für Smartphones und Tablets: Produkte im Überblick
- Welche Techniken stecken hinter KNOX für Android und wie kann in der Praxis damit umgegangen werden?
- Was leistet der Secure Workspace in Blackberry Balance?
- Wie unterscheiden sich diese Konzepte von Krypto-Phones, wie SiMKo 3?

Dominik Franke, ComConsult Beratung und Planung GmbH

14:45 Uhr
45 Minuten

WLAN-Security: Sichere Hotspots und Gastzugänge
- Gefährdungen in traditionellen Hotspots und Gastzugängen
- Sichere Authentisierung und Verschlüsselung in Hotspots und Gastzugängen: Geht das überhaubt?
- Hotspot 2.0 und Passpoint: Was steckt dahinter?
- Warum wir IEEE 802.1X nicht entkommen können

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

16:00 Uhr Ende der Veranstaltung

Das Kongressportal

Auf dem Kongressportal stellen wir Ihnen einige Hintergrundinformationen rund um die Themen des ComConsult IT-Sicherheits-Forum 2014 zur Verfügung.

Die markierten Beiträge sind spezielle Angebote, auf die ausschließlich Kongressteilnehmer Zugriff haben, um sich optimal auf die Veranstaltung vorzubereiten. Diese Seite wird laufend erweitert und aktualisert.

Nutzen Sie die Möglichkeit, bereits im Vorfeld der Veranstaltung Kommentare und Fragen zu den einzelnen Beiträgen abgeben und mit den Referenten über die Themen diskutieren zu können.

www.comconsult-research.de/kongresse/sicherheit-2014/

Schwerpunkthema

Data Center in a Box und die Folgen für die Informationssicherheit

Fortsetzung von Seite 1

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Dipl.-Inform. Sebastian Jansen hat Informatik mit dem Schwerpunkt „Verteilte Systeme“ an der RWTH Aachen studiert. Er ist Berater bei der ComConsult Beratung und Planung GmbH in den Bereichen Data Center und User-centric Communications. Dort beschäftigt er sich im Projektgeschäft mit den Themen Server-, Client- und Netzwerk-Virtualisierung, Storage und Unified Communications.

Dr. Melanie Winkler ist als Beraterin bei der ComConsult Beratung und Planung GmbH in dem Bereich IT-Sicherheit tätig. Dort beschäftigt sie sich besonders mit Sicherheitskonzeptionen nach ISO 27001 und BSI Grundschutz und deren Umsetzung.

Das Ergebnis in einem traditionellen, mit der Zeit gewachsenen RZ ist dann meist eine Heterogenität auf allen Ebenen, z.B. x86, AIX, Mainframe. Typisch ist außerdem eine starre hierarchische Vernetzung (Access, Aggregation, Core). Die Trennung von Mandanten erfolgt in Form von separaten Netzsegmenten, die über eine entsprechend leistungsfähige und hochverfügbare Data Center Firewall verbunden werden.

Eine solche komplexe und starre Struktur steht jedoch im Widerspruch zur Notwendigkeit schnell und flexibel Infrastrukturen für neue Mandanten, neue Dienste und Anwendungen bereitzustellen.

Horizontale Homogenisierung und Konsolidierung auf dem Vormarsch

Im modernen RZ wird daher eine Homogenisierung auf jeder Ebene durch einen möglichst hohen Konsolidierungsgrad angestrebt (Abbildung 1):

- Storage: Block- und File-basierte Zugriffe werden vom gleichen System bedient.
- Compute: Möglichst alle Dienste sollen per Virtualisierung auf x86-Server-Hardware abgebildet werden.
- Netzwerk: LAN & SAN konvergieren.
- Sicherheitsfunktionen rücken stärker an die Schutzobjekte und sind über die einzelnen Ebenen verteilt.

Die Vorteile dieses Konzepts liegen auf der Hand. So erreicht man innerhalb der einzelnen Ebenen eine hohe Flexibilität und Dynamik, da ein Verschieben innerhalb dieser Ebene beliebig möglich ist. Gleichzeitig reduziert die stark homogenisierte Hardwarelandschaft die Wartungs- und Schulungskosten, weil nun nicht mehr verschiedenste Plattformen adressiert werden müssen. Dem entgegen steht eine höhere Hardwarebindung und damit Herstellerabhängigkeit, durch eben jene Homogenisierung, sowie die Notwendigkeit an einigen Stellen Kompromisse und ggf. Einschränkungen die Funktionalität betreffend eingehen zu müssen. Konnte man durch die früheren Best-of-Breed-Ansätze die benötigte Funktionalität beliebig zusammenfügen, muss man sich jetzt auf einen gemeinsamen Nenner einigen.

RZ-Automatisierung und die Konsequenzen

Schlüsselthema im modernen RZ ist die Automatisierung, d.h. die automatische Provisionierung von VMs auf Virtualisierungs-Hosts und der dynamische Lastausgleich zwischen Virtualisierungs-Hosts.

Hierzu darf die Einrichtung und Zuweisung eines neuen Dienstes, einer neuen Applikation keine physikalische Änderung der Infrastruktur erfordern. Die physikalische Infrastruktur muss daher von Diensten, Applikationen und damit den logischen Strukturen so weit entkoppelt werden, dass die Einrichtung (das „Provisioning“) von Diensten und Applikationen ausschließlich auf der logischen Ebene erfolgen kann.

Dies erfordert zunächst den konsequenten Einsatz von Virtualisierungstechniken auf allen Ebenen der RZ-Infrastruktur, d.h. Virtualisierung in den Bereichen Compute / Server, Netzwerk und Storage. Hierdurch wird eine Konsolidierung und Vereinheitlichung der Infrastruktur sowie die Schaffung der notwendigen Verfügbarkeit und Kapazität bedingt.

Letztendlich stellt sich die gesamte Logik

Data Center in a Box und die Folgen für die Informationssicherheit

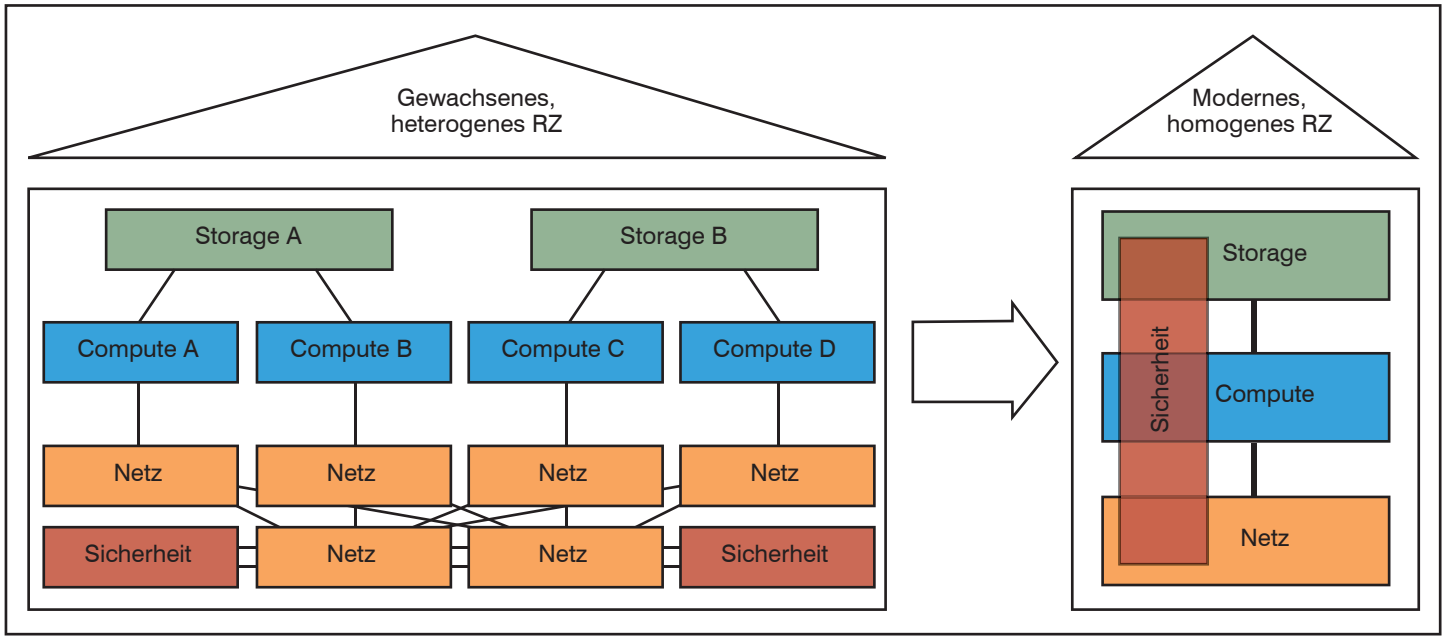


Abbildung 1: RZ-Evolution

im RZ als Software dar und die Konfiguration für einen neuen Server, eine neue Anwendung ist durch einen Satz von Scripts gegeben, der automatisiert abgearbeitet wird. Die Analogie zu Shell Scripts ist leider erschreckend, denn genau an dieser Stelle liegt die wesentliche Tücke.

Zunächst muss die Konfiguration übergreifend gesehen werden, d.h. neben VMs müssen Netzverbindungen und ggf. VLANs sowie Speicherbereiche eingerichtet werden. Diese Konfigurationen müssen natürlich zu den entsprechenden Vorgaben passen, die für den jeweiligen Mandanten relevant sind, und ein einziger Fehler in der Konfiguration kann (Sicherheits-)Vorfälle aller Couleur verursachen.

Erschwerend kommt hinzu, dass die Konsolidierung im Vergleich zum traditionellen Aufbau nur auf den ersten Blick zu Vereinfachungen führt, denn das Gegenteil ist der Fall. Die Struktur der Ebenen vereinfacht sich zwar auf Ebene der Hardware, auf Ebene der Software explodiert die Komplexität jedoch förmlich.

Demzufolge sind die eigentlich entscheidenden Aspekte im modernen RZ:

- Die Scripts, welche die RZ-Automatisierung steuern, sind als höchstkritische Software einzustufen, deren Qualität das A und O der RZ-Automatisierung ist.

- Striktes Configuration Management und Change Management in Verbindung mit einer lückenlosen Dokumentation und Revisionskontrolle der Konfigurationen sind ein absolutes Muss.

- Die Überwachung hinsichtlich (Security) Incidents muss im Vergleich zum traditionellen RZ viel genauer erfolgen.

2. Einfluss von integrierten Referenzarchitekturen und Fertiglösungen

Zusätzlich zu der eben beschriebenen horizontalen Homogenisierung gibt es aktuell einen weiteren Trend: die vertikale Integration.

Um eine horizontale Homogenisierung schrittweise, schneller und effektiver zu erreichen, und den o.g. Anforderungen nach stärkerer Konsolidierung nachzukommen, bieten verschiedene Hersteller seit einiger Zeit als Alternative das sogenannte Datacenter in a Box an. Hierbei handelt es sich um All-in-One-Lösungen bei denen Server, Netzwerk und Storage nicht länger getrennt, sondern als eine Einheit betrachtet und geliefert werden. Ein zentrales Management vervollständigt das Data Center in a Box. BITKOM spricht hier von **Vertikal integrierten Systemen (ViS)**[1].

Der Vorteil für den Kunden liegt dabei z.B. darin, dass er nicht mehr auf die Kompatibilität der einzelnen Komponenten untereinander schauen muss, da die Hersteller dieser Box-Lösungen diese im Vorfeld validiert haben. Dies verkürzt entsprechende Testphasen bei der Einführung neuer Systeme und erleichtert das Patch-Rollout. Gleichzeitig wird durch den Kauf einer Fertiglösung bzw. einer Referenzarchitektur mit identischer Hardware, ein hoher Skalierungs- und Konsolidierungsgrad auf allen Ebenen (Compute, Network, Storage) erreicht, was zu einer spürbaren Kostenersparnis führt und den Einsatz im Cloud-Bereich attraktiv macht. Der Preis ist allerdings eine starke Herstellerbindung.

2.1 Bedeutung im RZ-Umfeld

Betrachtet man das Konzept dieser Komplettpakete unter dem Aspekt einer ständig wachsenden Komplexität bei Konfiguration und Planung moderner Rechenzentren, wird die Bedeutung aufeinander abgestimmter Hardware erst richtig deutlich. So ist für die Kompatibilität eines Systems zu einem bestimmten Anwendungsszenario (sei es z.B. als Virtualisierungs-Host oder als Datenbankserver) heute nicht mehr ausreichend, dass eine bestimmte Leistungsklasse bei CPU oder Speicher erreicht wird. Vielmehr garantieren die jeweiligen Softwarehersteller die korrekte Funktionsweise ihrer Produkte ausschließlich mit explizit genannten Hardwarekomponenten. Dieser Umstand erschwert die Planung und erfordert deutlich mehr Absprachen und Abstimmung der Serverkomponenten aufeinander und auf die zu betreibenden Anwendungen und zukünftigen Anwendungsgebiete.

Hier spielen Referenzarchitekturen und Fertigsysteme ihre Stärke aus, nehmen Kompatibilitätssorgen und bieten Planungssicherheit. Auch den etwas höheren Preis und die vermeintliche Bindung an einen Hardwarehersteller (die de facto durch den Kauf herkömmlicher Rack- oder Blade-Systeme ebenfalls für eine gewisse Zeit gegeben ist), werden manche RZ-Betreiber dafür gerne in Kauf nehmen.

[1]Siehe https://www.bitkom.org/files/documents/131122_Whitepaper_ViS_Web.pdf

Während klassische Rack-Server und Blade-Systeme in naher Zukunft zwar sicher nicht aus den Rechenzentren verschwinden werden, kann man wohl davon ausgehen, dass die Zahl der integrierten Architekturen zunehmen wird. Werfen wir daher einen Blick auf die Konzepte der verschiedenen Hersteller in diesem Bereich.

2.2 FlexPod

Der FlexPod als Referenzarchitektur ist das Produkt einer Kollaboration von Cisco und NetApp für den Betrieb virtueller Server auf einer Integrierten Lösung. Während Cisco mit dem Unified Computing System (UCS) die eigentlichen Server und mit Produkten der Nexus-Reihe auch die Netzwerkanbindung stellt, liefert NetApp die entsprechenden „Unified Storage"-Komponenten. Für die Virtualisierung kann der Kunde auf VMware vSphere, Microsoft Hyper-V oder im Falle eines VDI-Betriebs auf Citrix Xen Desktop zurückgreifen. Da es sich nicht um eine 100% Fertiglösung, sondern um eine Referenzarchitektur handelt, kann der Kunde allerdings entsprechend seiner Bedürfnisse und Aufgaben aus verschiedenen Komponenten wählen. Das FlexPod-Konzept definiert in diesem Fall das Verhältnis von Server- zu Switch- und Storage-Zahlen und gibt Konfigurationen für die genutzten Komponenten und das zentrale Management vor. Neben den verschiedenen Einsatzszenarien als universeller Virtualisierungs-Host existieren auch spezielle Konfigurationen für SAP-Applikationsserver und diverse Cloud-Lösungen.

Durch die zentrale Management-Komponente erlaubt die FlexPod-Architektur einerseits die einfache Einbindung in existierende externe Management-Systeme.

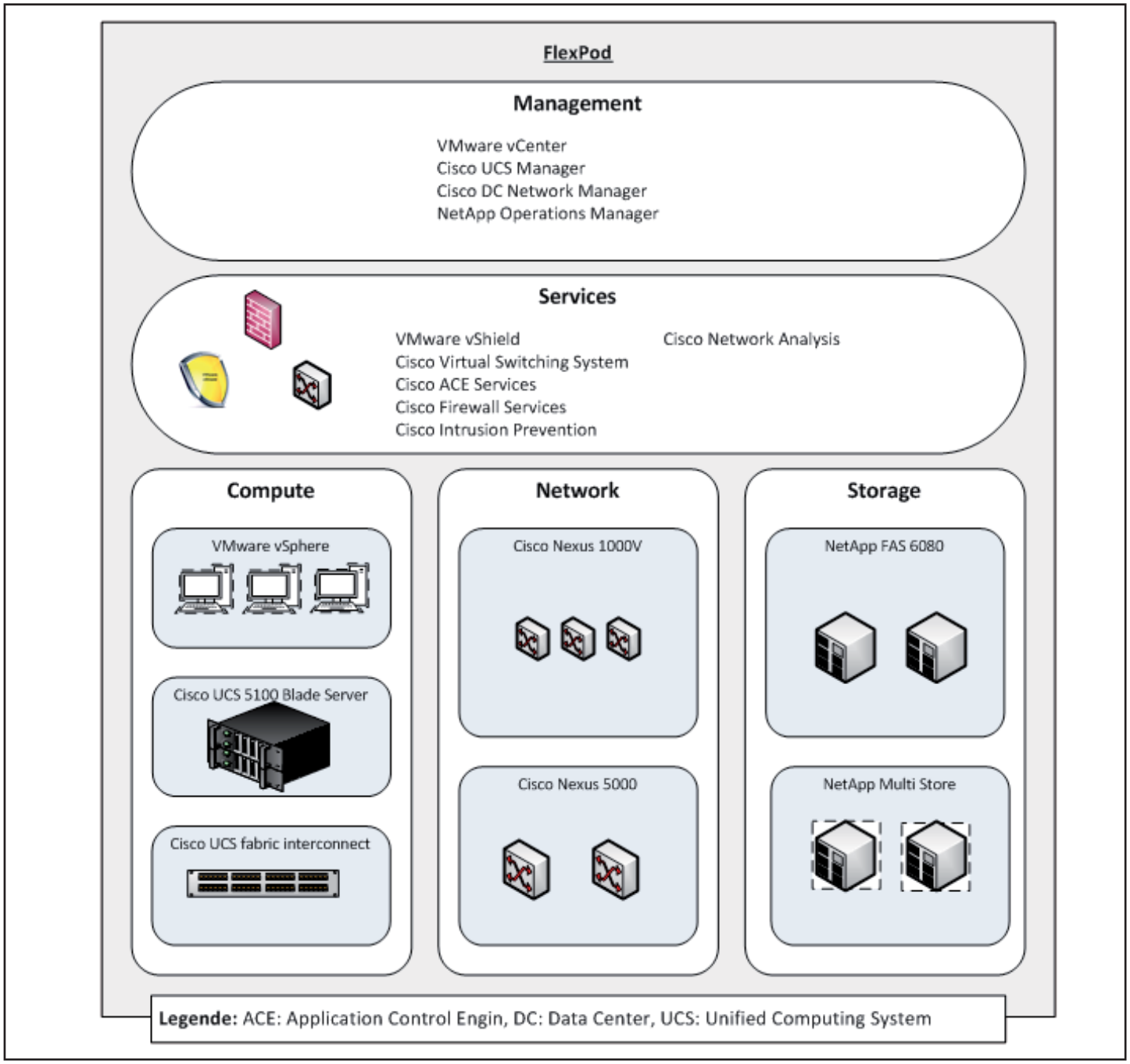


Abbildung 2: Komponenten im FlexPod

Andererseits ermöglicht die Architektur aber auch, durch das Pooling von Ressourcen, eine starke Automatisierung und Orchestrierung innerhalb einzelner bzw. übergreifend auch zwischen verschiedenen FlexPods. Darüber hinaus ermöglicht das zentrale Management ein einfaches Ausrollen von Patches und bietet einen Gesamtüberblick über den Status aller Komponenten des Systems.

2.2.1 Netzanbindung
Im Vergleich zu herkömmlichen Rack- oder Blade-Lösungen erfolgt bei der FlexPod-Architektur keine Anbindung der einzelnen Komponenten an das jeweilige Daten- bzw. Storage-Netz. Stattdessen aggregiert eine „Fabric Interconnect"-Komponente (z.B. Cisco 6100er bzw. 6200er Switches) den gesamten Pod in einer gemeinsamen Backplane. Das bedeutet, sowohl Daten- als auch Storage-Traffic laufen zusammen über diese gemeinsame Komponente. Somit sind alle Komponenten des FlexPod mit 10GE angebunden. Innerhalb des FlexPod bedeutet dies gleichzeitig auch eine Konvergenz des Datenverkehrs auf gemeinsamen Komponenten. (siehe Abbildung 2)

2.2.2 Mandantenfähigkeit
Mandantenfähigkeit ist ein Schwerpunkt beim Entwurf der FlexPod Referenzarchitektur. Als bisher einziges ViS bietet FlexPod dabei mit Secure Multi-Tenancy (sichere Multi-Mandantenfähigkeit) ein System, das sowohl die Sicherheitsstandards der Payment Card Industries (PCI), der Homeland Security der USA sowie der International Computer Security Association (ICSA) Audits erfüllt.

Diese Mandantenfähigkeit beruht beim FlexPod auf vier Säulen:

- **Verfügbarkeit** – Diese Säule garantiert die Verfügbarkeit der einzelnen Komponenten des Systems, auch im Fehlerfall. Erreicht wird dieses Ziel durch diverse Hochverfügbarkeitsmaßnahmen innerhalb der Systemkomponenten.

- **Sichere Trennung** – Auf Ebene der Einzelkomponenten wird dafür Sorge getragen, dass die Mandanten zuverlässig voneinander separiert sind. Dies erfolgt durch den Einsatz von Virtualisierung (VLANs, Virtual Storage Controller, virtuellen Firewalls, etc.) und Zugriffskontrollmechanismen. Die einzelnen Schichten nutzen dabei ihre jeweiligen Techniken, um diese Trennung auch im Rahmen angrenzender Schichten sicherzustellen.

- **Service-Garantie** – Im Gegensatz zur reinen Verfügbarkeit, sichert diese Säule den jeweiligen Mandanten voneinander getrennte Dienste mit bestimmten QoS-Parametern zu. Dies beinhaltet sowohl eine bestimmte Netzwerkbandbreite als auch Rechenleistung und Speicherplatz auf dem Storage-System.

- **Management** – Das Management bildet schließlich den zentralen Punkt der Konfiguration und erlaubt, den jeweiligen Mandanten schnell weitere Ressourcen zuzuweisen bzw. auf einfachem Wege neue Ressourcen zu provisionieren. Mit Hilfe zentraler Schnittstellen und APIs steuert das zentrale Management dabei die jeweiligen spezifischen Management-Tools der Einzelkomponenten.

Die Architektur-Komponenten des FlexPods zielen darauf ab, den Erhalt der genannten Punkte zu gewährleisten. Um eine flexible Nutzung des Systems zu ermöglichen, werden die zur Verfügung stehenden Komponenten jedoch weiter in zwingend erforderliche Kernkomponenten sowie flexibel auswählbare Mandanten-bedingte Komponenten unterteilt. Auf diese Weise kann die Mandantenfähigkeit, bei gleichzeitiger Anpassungsfähigkeit an Kundenbedürfnisse und die Flexibilität des Systems, garantiert werden.

2.3 Vblock

Virtual Computing Environment Company ist eine amerikanische Firma, die 2011 aus einem Joint Venture zwischen Cisco und EMC mit weiteren Investitionen durch VMware und Intel entstand. Mit dem als Vblock bezeichneten System bietet VCE (Virtual Computing Environment) ihre Version eines integrierten Systems. Wie beim FlexPod liefert Cisco auch beim Vblock Rechenleistung und Netzwerkkomponenten, während die Storage-Komponenten hier von EMC kommen. Darüber hinaus läuft ein VMware Hypervisor auf dieser Hardware und macht den Vblock zum Virtualisierungs-Host. Auch hier rundet ein zentrales Management das Paket ab. Darüber hinaus dient VCE auch als zentraler Dienstleister für Wartung und Support.

Der Vblock ist in verschieden leistungsfähigen Ausführungen erhältlich. Im Gegensatz zur Referenzarchitektur des FlexPods handelt es sich hierbei jedoch um eine Fertiglösung, sodass keine freie Konfiguration des Systems möglich ist.

Wie bereits erwähnt, besteht der Vblock aus Komponenten von Cisco, EMC, Intel und VMware. Den Kern, also die eigentliche Rechenleistung liefern Cisco UCS Blade-Server, die über Cisco Fabric Interconnect und Fabric Extender angebunden sind. Im Netzbereich kommen diverse Cisco Switches der 5000er-, 7000er und 9000er-Reihe zum Einsatz. Darüber hinaus setzt Cisco auf Ebene der Virtualisierungs-Hosts den virtualisierten Switch Nexus 1000V ein. Storage liefert schließlich das EMC Symmetrix System, das wahlweise rein blockbasiert oder als Unified Storage, d.h. sowohl block- als auch dateibasiert, genutzt werden kann. Die Virtualisierung ist mittels VMware vSphere, inkl. des passenden vCenter-Servers realisiert.

Das Management des Vblock teilt sich in zwei Teile. Zum einen bietet VCE Vision Intelligent Operations Zugriff auf die System-Bibliotheken und Management-Tools für das gesamte System, während ein zweiter Block es ermöglicht, die einzelnen Komponenten zu administrieren.

2.3.1 Netzanbindung
Netzwerk-seitig bietet VCE zwei Varianten. Während bei einer separierten Netzwerkkonfiguration Cisco 5000er- bzw. 7000er-Switches im LAN-Bereich sowie SAN-Switches der 9000er-Serie im Storage-Bereich zum Einsatz kommen, gibt es auch die Möglichkeit des Betriebs mittels eines Unified Networks. In diesem Fall entfällt die Trennung zwischen SAN und LAN und der komplette Netzwerk-Traffic läuft über ein einzelnes Paar von Cisco 5500er Switches.

Vblock erlaubt außerdem den Zusammenschluss mehrerer getrennter Vblock-Systeme. Durch den Einsatz von Cisco (SAN-) Switches werden so Hochverfügbarkeitsdienste, wie Migration, Replikation, Backup und Desaster Recovery ermöglicht. Gleichzeitig bietet diese Aggregationsebene aber auch einen gemeinsamen Zugriffspunkt auf externe Netze und umgekehrt (siehe Abbildung 3).

2.3.2 Mandantenfähigkeit
Auch VCE setzt mit Vblock auf Mandantenfähigkeit. Die Vblock Solution for Trusted Multi-Tenancy (TMT) basiert dabei auf sechs Teilen:

- **Secure Separation** beschreibt die zuverlässige Trennung der einzelnen Mandanten durch den gezielten Einsatz unterschiedlicher Sicherheitsmaßnahmen. Trotz der gemeinsamen Nutzung diverser Ressourcen soll so sichergestellt werden, dass die einzelnen Mandanten jeweils nur Zugriff auf ihre eigenen Ressourcen haben (siehe Abbildung 4).

- **Service Assurance** beschreibt die Zusicherung und Bereitstellung der verschiedenen Ressourcen für die auf dem System beheimateten Mandanten. Mittels der jeweils hauseigenen QoS-Mechanismen auf den einzelnen Ebenen des Systems (Cisco UCS, EMC Symmetrix, VMware vSphere) und virtuellem Ressourcenpooling werden so entspre-

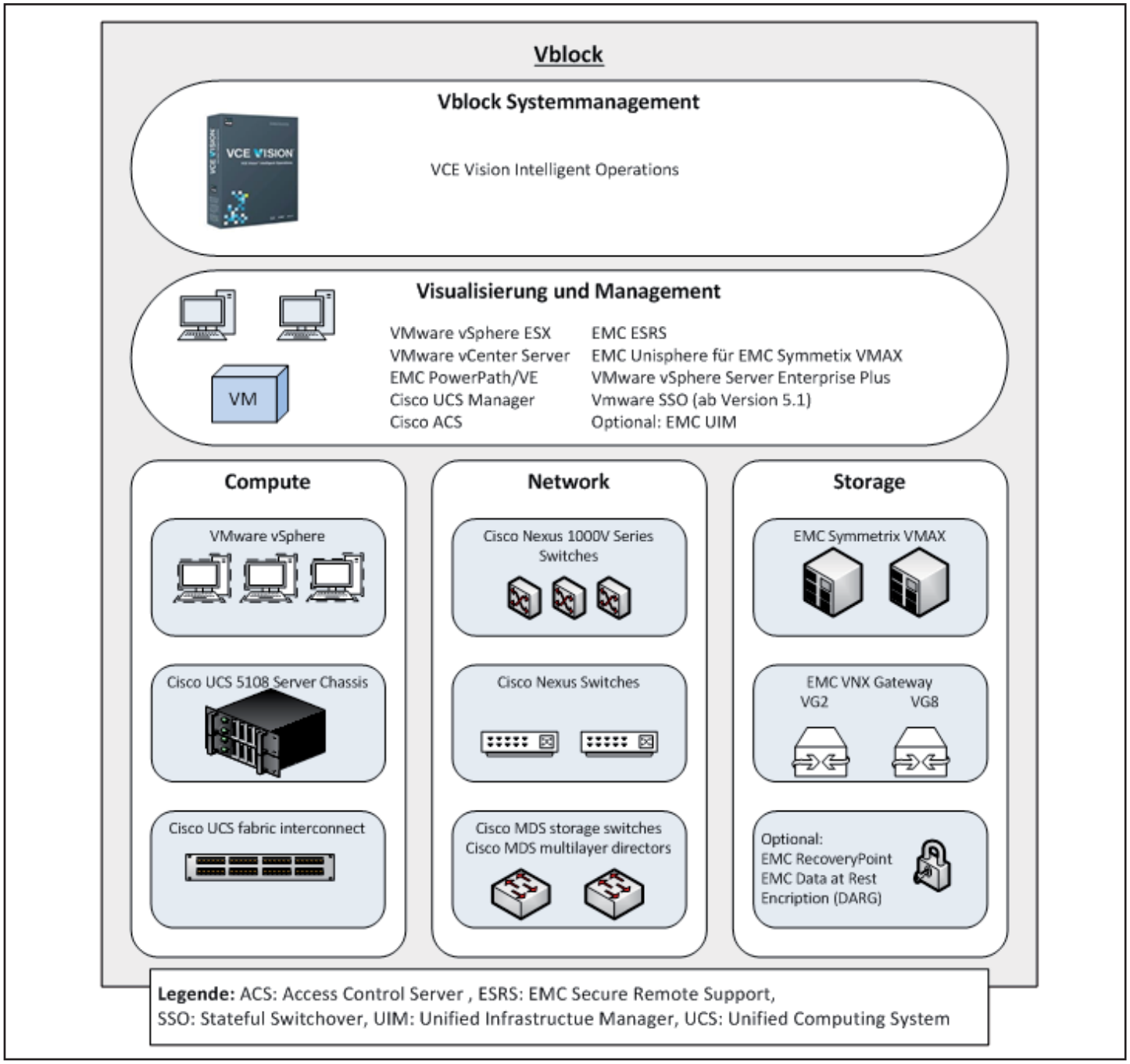


Abbildung 3: Komponenten im Vblock

chend der vereinbarten SLAs Ressourcen verteilt und ggf. neu allokiert.

- **Security and Compliance** stellt, im Gegensatz zu Secure Separation, nicht die Trennung der einzelnen Mandanten in den Vordergrund, sondern legt den Fokus auf die Sicherheit der jeweiligen Daten. Dabei rücken Aspekte wie Zugriffskontrollen, Verschlüsselung und Schlüsselverwaltung, Management-Sicherheit, aber auch Monitoring, Recording und Verifikation der Vorgänge auf dem System in den Mittelpunkt.
- **Availability and Data Protection** beinhaltet neben der Redundanz der entsprechenden Systeme den Schutz der gespeicherten Daten und entsprechende Backup-Lösungen.
- **Tenant Management and Control** umfasst die Möglichkeit der teilweisen Selbstverwaltung von Ressourcen und virtuellen Systemen durch den jeweiligen Mandanten (eng. tenant). Dies reduziert einerseits den Aufwand an zentraler Verwaltung und räumt gleichzeitig den Mandanten Freiheiten bei der Kontrolle und Administration der eigenen Systeme ein. Andererseits beinhaltet dieser Punkt aber auch die Sicherung der Verwaltung dahingehend, dass Mandanten ausschließlich in der Lage sind, ihre eigenen Systeme und Daten zu verwalten.
- **Service Provider Management and Control** beinhaltet Funktionen, damit der Service Provider, die verschiedenen Mandanten auf seinem System entsprechend ihrer jeweiligen SLAs betreuen und verwalten kann. Hierzu zählen z.B.

Data Center in a Box und die Folgen für die Informationssicherheit

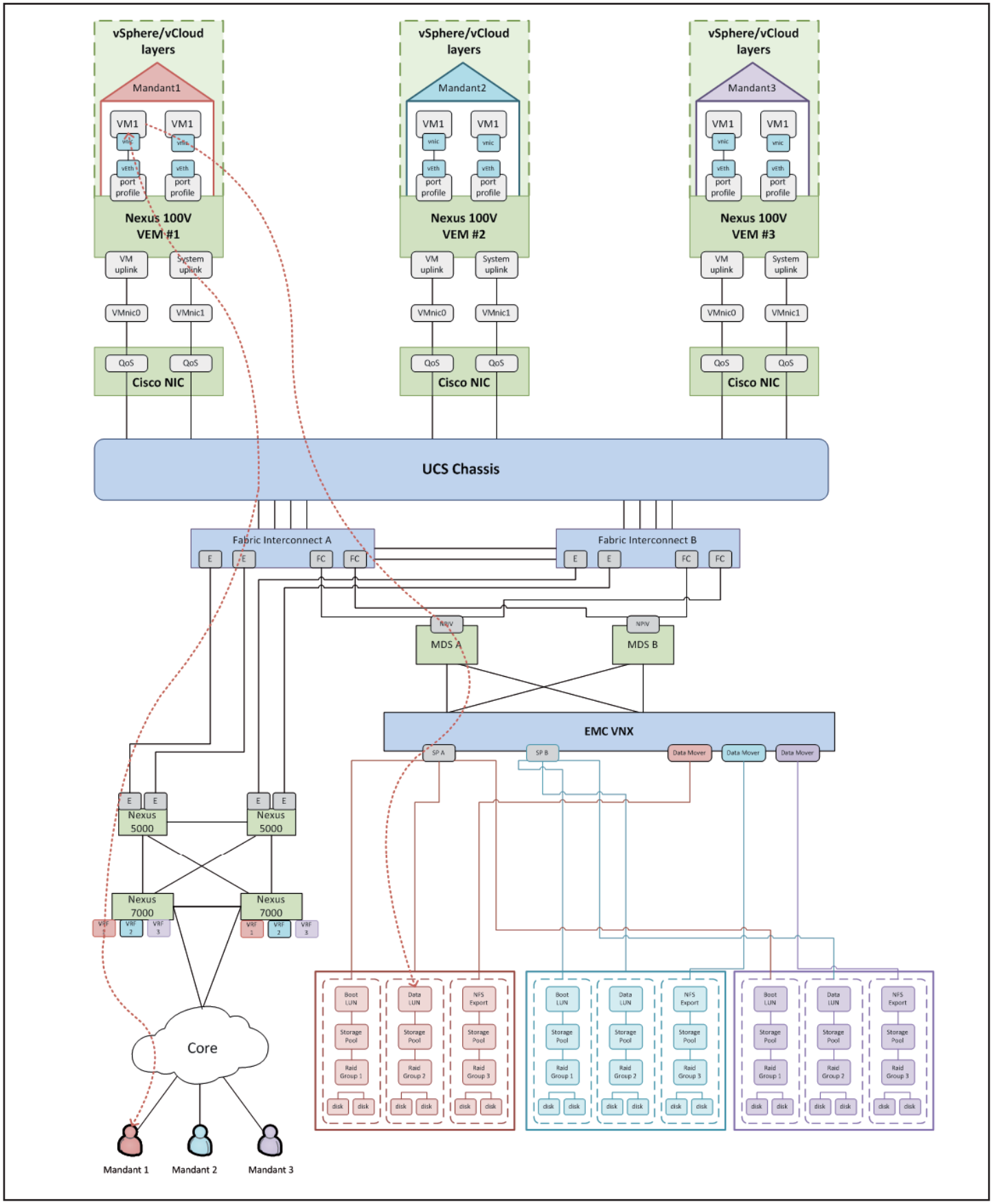


Abbildung 4: Mandantentrennung in Vblock[2]

[2]Siehe http://www.vce.com/asset/documents/tmt-design-guide.pdf

ausführliche Monitoring- und Alarm-Systeme, aber auch Werkzeuge zur schnellen (De-)Provisionierung von Pooled Ressources an bestimmte Mandanten.

2.4 IBM PureSystems

Wie auch der Vblock stellt die PureSystems Familie von IBM eine Datacenter-in-a-box-Lösung dar, bei der alle Komponenten vorinstalliert werden. Ein Hauptunterschied zu den beiden bisherigen vorgestellten Konzepten liegt darin, dass bei IBM die komplette Hardware aus einer Hand kommt. Während bei den anderen Systemen Cisco verschiedene Kollaborationen mit Speicherherstellern einging, sind hier also sowohl Server als auch Netz- und Storage-Komponenten von IBM selbst. Als Virtualisierungslösung können hier die verschiedenen Hypervisoren der gängigen Hersteller zum Einsatz kommen. Auch dieses System bietet ein zentrales Management zur einfachen Administration.

Die Mitglieder der PureSystems-Familie kommen dabei in unterschiedlichen Ausprägungen daher. So zielt der PureFlex hauptsächlich auf den Einsatz im Cloud- bzw. IaaS-Bereich (Infrastructure as a Service) ab. Daneben gibt es noch Varianten als Applikations-Server sowie Datenbank-Server und die Möglichkeit, das System selbst an die Bedürfnisse anzupassen. Damit stellt PureSystems einen Mittelweg zwischen der FlexPod-Referenzarchitektur und der Komplettlösung á la Vblock dar.

2.4.1 Netzanbindung

Netzwerkseitig bieten die verschiedenen Konfigurationen diverse Standards und Vorgehensweisen der Anbindung. Auf der einen Seite bietet das System den Einsatz von Converged Networking Komponenten zur gleichzeitigen Anbindung von Speicher und Netz über dieselbe Hardware. Die Speicheranbindung würde in diesem Fall mittels FCoE (Fiber Channel over Ethernet) realisiert.

Andererseits ist es, dem klassischen Ansatz folgend, ebenso möglich diese beiden Teile über getrennte Hardware anzubinden. Dann steht für die Storage-Anbindung FC und für die herkömmliche Netzanbindung, zusätzlich zu Ethernet, auch Infiniband zur Verfügung.

Neben einer möglichen internen Trennung des Datennetzes nach Mandanten, erfolgt außerdem eine Unterteilung in drei gesonderte VLANs. Das erste Netz umfasst dabei das Managementnetz für Hardware und Hypervisor. Das zweite Netz stellt die herkömmliche Netzanbindung dar. Diese beiden Netze sind auch entsprechend an das externe Netz angebunden. Das dritte VLAN hingegen ist ein rein internes Netz (d.h. ohne Verbindung in das restliche RZ-Netz) und erlaubt das Management des gesamten Systems aus dem internen Netz heraus.

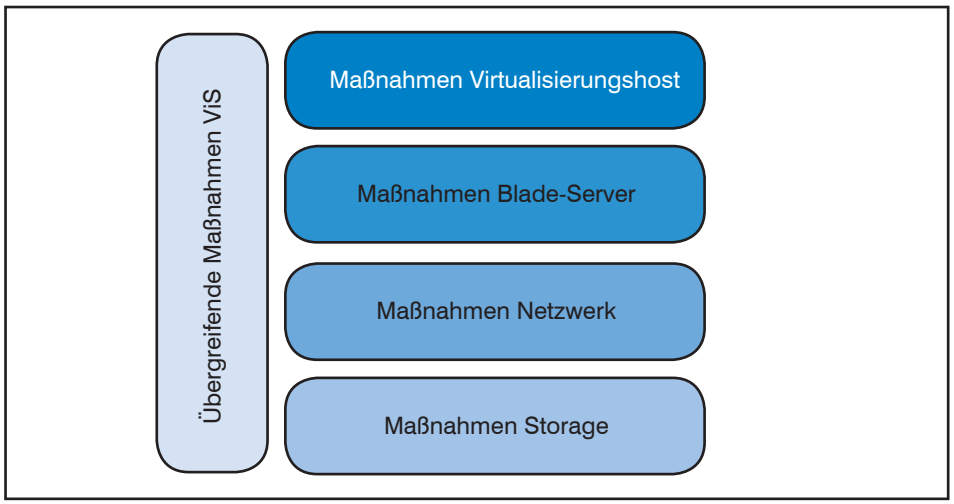


Abbildung 5: Elemente eines Sicherheitskonzepts für ViS

Insgesamt führt dies dazu, dass das Pure System an das externe Speichernetz, an das Datennetz des RZs sowie - im Falle einer zu erwartenden Trennung des Managementnetzes - an ein zusätzliches Managementnetz angebunden ist und somit in drei Netzen eingebunden ist.

2.4.2 Mandantenfähigkeit

Auch PureSystems und speziell die Cloud-orientiere PureFlex-Variante bieten eine Mandantenfähigkeit und ebenso wie bei den anderen Vertretern der ViS-Kategorie liegt hier der Schwerpunkt auf Trennung der Systeme mittels Servervirtualisierung und Trennung der Netze durch VLAN-Bildung. Zusätzlich setzt IBM mit Corents Multi-Tenant Server und SaaS Cockpit (Software as a Service) auf eine Lösung zur Etablierung von SaaS auf Basis des PureSystems. Diese Softwarelösung erlaubt den Betrieb von Einzel-Mandantenapplikationen als Multi-Tenant-Anwendung auf den Modellen der PureSystems. Dazu beinhaltet das System u.a. Werkzeuge zur Verwaltung und Provisionierung von Mandanten, zum Monitoring der aktuellen Auslastung und den aktuell genutzten Applikationen sowie zur Abrechnung. Dieses System ist allerdings kein integraler Bestandteil der Lösung, sondern setzt auf der eigentlichen PureSystem-Lösung auf.

3. Integrierte Sicherheitskonzepte für Vertikal integrierte Systeme

Vertikal integrierte Systeme sind zunächst denselben Gefährdungen ausgesetzt, die sich analog zu horizontaler Homogenisierung durch den Einsatz von Virtualisierungstechniken im Server- und Client-Bereich im Netz- und im Storage-Bereich ergeben.

Darüber hinaus sind jedoch durch das Zusammenwirken der Ebenen ganzheitliche Aspekte zu berücksichtigen, die speziell im Bereich der Automatisierung besonders ausgeprägt sind. Die Gesamtkonfiguration für einen einzelnen Mandanten, die ja haarklein ebenenübergreifend aufeinander abgestimmt werden muss, ist hochgradig komplex und deshalb ausgesprochen fehleranfällig.

Die wesentliche Gefährdung ist klar: Winzigste Fehler können das gesamte Gebilde signifikant stören und das Trouble Shooting könnte sich als kaum noch durchführbar erweisen. Gerade letzteres ist in der täglichen Praxis ein sehr großes Problem. Wenn Fehler auf Software-Ebene, z.B. in der logischen Trennung, in Regelwerken von Firewalls vorliegen, fehlen oft die Werkzeuge zur effektiven Fehlersuche, da ein Fehler sich ja ggf. erst ebenen- und damit produktübergreifend zeigt.

Management, Überwachung und Trouble-Shooting müssten also produktübergreifend für die gesamte Data-Center-Box funktionieren. Auch wenn Data-Center-in-the-Box-Systeme im Vergleich zu anderen Konzepten am ehesten die Möglichkeit haben eine solche vereinheitlichte Gesamtsicht zu schaffen, ist die Realität zumindest aktuell noch nicht besonders erfreulich.

Während wir im Bereich der eigentlichen Software-Entwicklung erheblich dazugelernt haben, was Verifikation und Validierung von kleinsten Code-Schnipseln bis zum Gesamtsystem im gesamten Entwicklungsprozess anbelangt, sind wir bei Scripts und Konfigurationen in der modernen IT (die ja auch Software sind) anscheinend noch in den Kinderschuhen.

Die Sicherheitsmaßnahmen für das Data Center in a Box müssen also nicht nur die einzelnen Ebenen adressieren (was ja eigentlich nicht viel Neues darstellen würde) sondern speziell auch übergreifende Aspekte berücksichtigen, welche die Box in ihrer Gesamtheit und die Interaktionen zwischen Boxen betrachten (siehe Abbildung 5). Dies zeigt insbesondere auch eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgebrachte Studie für Vblock, welche die Gefährdungen analysiert und entsprechende Sicherheitsmaßnahmen spezifiziert[3].

3.1 Maßnahmen Virtualisierungs-Host

Grundsätzlich führt die Verkettung aus physischem und virtuellem System im ersten Schritt sowohl aufgrund der Architektur als auch aufgrund der zusätzlichen Komplexität zu einem geringeren Sicherheitsniveau, da ein Mehr an Software-Komponenten auch ein Mehr an denkbaren Schwachstellen bedeutet. Eine detaillierte Gefährdungsanalyse kann in den IT-Grundschutz-Katalogen[4] des BSI dem Grundschutzbaustein B 3.304 „Virtualisierung“ entnommen werden. Für den Einsatz von Anwendungsvirtualisierung sind die Gefährdungen zum Grundschutzbaustein B 3.305 „Terminalserver“ relevant.

3.1.1 Server-Virtualisierung

Die Flexibilität und Dynamik der Server-Virtualisierung hat unmittelbare Auswirkungen auf die Auswahl der anzuwendenden Sicherheitsmaßnahmen.

Absicherung der Virtualisierungslösung

Eine Basis kann neben den allgemeinen Schutzmaßnahmen für Server insbesondere die Umsetzung der anwendbaren Maßnahmen des Bausteins B 3.304 „Virtualisierung“ der BSI IT-Grundschutz-Kataloge sein.

Um simultan Ressourcen für unterschiedliche Mandanten und allgemein Sicherheitszonen zur Verfügung zu stellen, muss die Virtualisierungslösung besonders gut gehärtet werden. Es wird empfohlen, hierzu pauschal eine Härtung für einen hohen Schutzbedarf durchzuführen. Für diesen Zweck können auch entsprechende Maßnahmenkataloge der Hersteller zu Rate gezogen werden.

Für VMware ist bei einem hohen Schutzbedarf beispielsweise zusätzlich zu den genannten Maßnahmen die Umsetzung des Maßnahmenkatalogs vSphere Hardening Guide[5] wie folgt sinnvoll (siehe auch Abbildung 6):

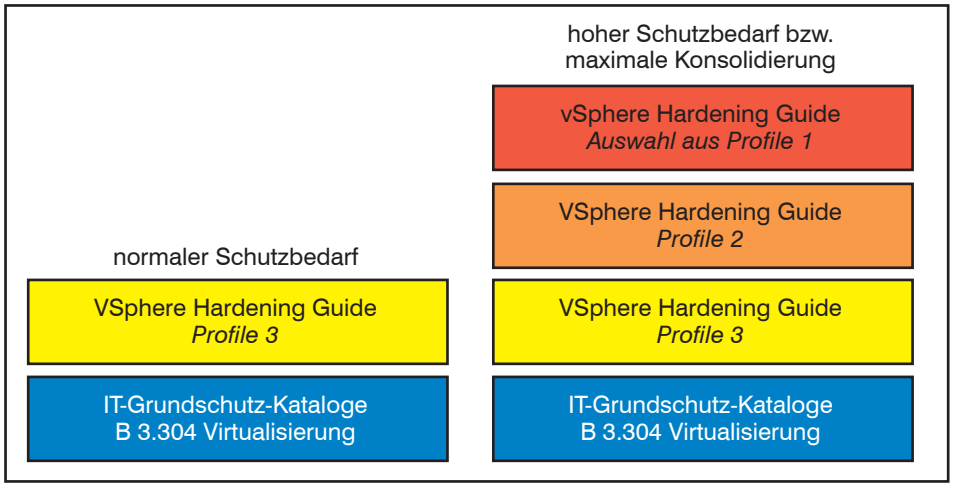


Abbildung 6: Absicherung von Virtualisierungslösungen

- Umsetzung aller anwendbaren Maßnahmen von Level 3, d.h. Maßnahmen für den normalen Schutzbedarf
- Umsetzung aller anwendbaren Maßnahmen von Level 2, d.h. Maßnahmen für exponierte Systeme und Systeme mit hohem Schutzbedarf
- Umsetzung ausgewählter Maßnahmen von Level 1, d.h. Maßnahmen für besonders schützenswerte Systeme

Normierung virtueller Server und Spezifikation zugehöriger Maßnahmenbündel

Wesentliches Element einer praktikablen sicheren Server-Virtualisierung ist die Normierung von zumindest denjenigen virtuellen Servern, die produktive Daten verarbeiten. Dies beinhaltet zunächst Konfigurationsvorgaben an das Betriebssystem auf den virtuellen Servern sowie die Festlegung der Anwendungsbereiche und der Dienste.

Für jeden derart normierten virtuellen Server wird ein Standardmaßnahmenbündel für den normalen Schutzbedarf (Mindesthärtung) sowie bei Bedarf ein hierauf aufbauendes erweitertes Maßnahmenbündel für den hohen Schutzbedarf festgelegt. Die wesentlichen Vorgaben werden dann als Konfigurationsrichtlinie für jedes Gastbetriebssystem festgelegt. Grundlage sind die Sicherheitsmaßnahmen für Server.

Einsatz virtualisierter Sicherheitskomponenten

Falls der Kommunikationsverkehr innerhalb eines Virtualisierungs-Hosts gefiltert werden muss (z.B. um die Kommunikation zwischen zwei VMs auf dem Virtualisierungs-Host zu kontrollieren) können folgende Alternativen in Betracht gezogen werden:

- Einsatz virtualisierter Sicherheitskomponenten (z.B. Firewall), die als VM und/oder als Komponente des Hypervisor bzw. eines virtualisierten Switches realisiert werden
- Einsatz von spezifischen externen Sicherheitskomponenten (z.B. Firewall), die mit einer Komponente des Hypervisor bzw. eines virtualisierten Switches kommunizieren und über diesen Weg auch den zu überwachenden Verkehr erhalten und Filterentscheidungen zurückmelden können[6]

3.2 Maßnahmen Anwendungs- und Desktop-Virtualisierung

Bei der Virtualisierung von Anwendungen und Desktops ist zu berücksichtigen, dass hiermit Client-bezogene Software-Komponenten (im Extremfall ein vollständiger Client als VM) im Rechenzentrum bereitgestellt und auch dort ausgeführt werden. Als Folge würde sich beispielsweise eine Infektion eines Desktops mit einer schadenstiftenden Software unmittelbar im Rechenzentrum auswirken können.

Absicherung einer Plattform für die Anwendungsvirtualisierung

Als Basis kann neben den allgemeinen Schutzmaßnahmen für Server die Umsetzung der anwendbaren Maßnahmen des Bausteins B 3.305 „Terminalserver“ der BSI IT-Grundschutz-Kataloge in Betracht gezogen werden.

Für bereitgestellte Anwendungen ist ein Virenschutz vorzusehen (z.B. Schutz gegen Makroviren). Terminal Server / VDI Server sollten für einen Mandanten zudem eigenen Sicherheitszonen zugeordnet werden (d.h. in separaten Netzen,

[3]Siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Cloud_Computing_Studie_Einsatz_VCE_Vblock.html
[4]Siehe https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
[5]Siehe http://www.vmware.com/support/support-resources/hardening-guides.html
[6]Auch als Service Insertion bezeichnet und bedeutet die Umleitung von Daten vom Hypervisor zu externer Einheit und zurück (Traffic Redirection).

kontrolliert durch eine Firewall) bzw. ggf. sogar einen eigenen Mandanten bilden.

Absicherung einer Virtual Desktop Infrastructure (VDI)

Da bei einer VDI-Lösung Clients als VM bereitgestellt werden können, ist die Umsetzung einer ggf. produktspezifischen Kombination der anwendbaren Maßnahmen der Bausteine B 3.304 „Virtualisierung“ und B 3.305 „Terminalserver“ der BSI IT-Grundschutz-Kataloge sinnvoll.

Für virtualisierte Clients sind die Sicherheitsmaßnahmen, die für physische Clients angewendet werden, sinngemäss zu übertragen. Dabei ist z.B. ein Virenschutz essentiell. Hierbei sind Besonderheiten einer VDI zu beachten. Ein simultaner Full System Scan mehrerer virtualisierter Clients kann in einem erheblichen Umfang Systemressourcen beanspruchen. Es kann daher für VDI in Betracht gezogen werden eine „Security VM“ einzusetzen, die auf einem Virtualisierungs-Host den Virenschutz durch spezielle Schnittstellen im Hypervisor zentral für alle VMs realisieren kann.

3.3 Maßnahmen Blade Server

Blade Server sind z.B. bei FlexPod oder Vblock mit UCS ein Bestandteil des Systems und müssen daher im Sicherheitskonzept entsprechend berücksichtigt werden. Für die Blades gelten zunächst weiterhin die Standardmaßnahmen für Server.

Die Zuordnung von Server zu Blade ist sehr flexibel und rein konfigurationsgesteuert. Hierdurch besteht die grundsätzliche Gefahr einer Fehlkonfiguration, die z.B. einen Server aus dem Bereich Entwicklung / Test dem produktiv genutzten Netzbereich zuordnen könnte. Ergänzend sollten daher folgende Maßnahmen für Blade Server in Betracht gezogen werden.

Serviceprofile

Die Provisionierung eines neuen Servers erfolgt durch ein Serviceprofil. In einem XML File sind alle Daten enthalten, die für die Identität relevant sind (BIOS-Version, Boot-Methode, Boot-Reihenfolge, MAC-Adressen, IP-Adressen, WWN, …). Serviceprofile werden per Template konfiguriert. Dabei werden z.B. MAC-Adressen aus einem Pool zugewiesen.

Besonders wichtig ist eine Qualitätssicherung der Templates / Serviceprofile durch Review, Inspection und Staging, d.h. Änderungen sollten möglichst zunächst nur in einem Template für den Bereich Entwicklung/Test erfolgen.

Weiterhin ist eine Aufnahme der Konfiguration (inkl. Template) in ein Configuration Management (CM) und Change Management zu empfehlen. Dies beinhaltet

- Versionierung der Konfiguration von z.B. UCS über ein CM-Tool
- „Anheften“ der UCS-Konfiguration an Changes im jeweils verwendeten Ticketing-System (z.B. Remedy).

Außerdem ist sicherzustellen, dass keine ungeplanten Änderungen an einem Serviceprofil stattfinden.

- Über ein Berechtigungskonzept kann grundsätzlich erreicht werden, dass nur speziellen Administratoren das Erstellen / Ändern von Templates und Pools sowie andere kritische Operationen erlaubt werden. Wenn ein solches Konzept nicht über das verwendete Blade-System realisiert werden kann, muss organisatorisch per 4-Augen-Prinzip vorgegangen werden.
- Auf Ebene des verwendeten Blade-Systems (z.B. UCS) kann üblicherweise verhindert werden, dass geänderte Templates und Serviceprofile automatisch oder versehentlich aktiviert werden.

Administration und Überwachung

Bei UCS erfolgt beispielsweise die Administration einer Fabric Interconnect mit der Java-Anwendung UCS Manager. Mit UCS Central wird die Gesamtadministration über alle UCS Manager ermöglicht. Der administrative Zugriff kann gegen ein Verzeichnis (z.B. AD oder LDAP) authentisiert werden. Wie auch in anderen Bereichen zu empfehlen, sollten für administrative Zugriffe personenbezogene Konten genutzt werden. Ein administrativer Zugriff sollte auf HTTPS beschränkt werden. Telnet ist bei UCS zwar standardmäßig deaktiviert, HTTP muss jedoch manuell deaktiviert werden.

Die Überwachung der Blades kann über eine bereits etablierte Standardüberwachung von Servern erfolgen (z.B. über Werkzeuge wie eHealth und Spectrum). Außerdem kann das Blade-System (z.B. UCS) auch SNMP-Traps senden.

Darüber hinaus ist eine Protokollierung auf dem Blade-System eine sinnvolle Maßnahme. Für UCS gilt hier, dass für das UCS Logging die System Event Log Policy (SEL Policy) für das Blade Server Log so konfiguriert werden muss, dass regelmäßig eine Übertragung des Blade Server Log erfolgt und die Inhalte anschließend gelöscht werden. Ohne diese Konfiguration läuft das Log schnell voll und wird nicht mehr neu beschrieben.

3.4 Maßnahmen Netzwerk

Die Switches in einer ViS-Lösung sind natürlich genauso abzusichern wie die sonstigen Switches im Netz. Dies gilt insbesondere für virtualisierte Switches (zum Beispiel Microsoft Extensible Virtual Switch, VMware vSwitch, Cisco Nexus 1000V).

Als Grundlage können hier die Maßnahmen der BSI IT-Grundschutz-Kataloge aus dem Baustein B 3.302 „Router und Switches“ dienen.

3.5 Maßnahmen Storage

Auch für ViS-Lösungen sind zunächst Standardsicherheitsmaßnahmen auf die verwendete Storage-Lösung anzuwenden (z.B. der Maßnahmenkatalog aus Baustein B 3.303 „Speichersysteme und Speichernetze“ der BSI IT-Grundschutz-Kataloge).

Bei der Nutzung eines Storage Area Network (SAN) in einer ViS-Lösung wie Vblock besteht grundsätzlich ein Kurzschlussrisiko zwischen unterschiedlichen Mandanten (d.h. ein unberechtigter Zugriff eines Mandanten auf den Speicher eines anderen Mandanten), das allerdings durch eine geeignete Zonierung mit SAN-Bordmitteln verhindert werden kann. Bei SANs auf Basis von Fiber Channel (FC) besteht zusätzlich noch eine technologiebedingte starke Trennung zwischen IP-Netzen und SANs. Bei FC over Ethernet (FCoE) hängt das Risiko von der Netzkonfiguration ab. Werden Switches exklusiv für FCoE genutzt, ist man aus einer Sicherheitsperspektive wieder recht nah an FC herangerückt. Andernfalls müssen auf den Switches zusätzliche Sicherheitsmaßnahmen umgesetzt werden, um das Risiko zu minimieren.

Interessanter ist da schon die NAS-Anbindung, die z.B. bei FlexPod zum Einsatz kommt. NAS Filer werden hier von mehreren Mandanten (bzw. Sicherheitszonen) genutzt. NAS Filer sind dann als Multihomed Server zu behandeln und für den Mandantenbetrieb spezifisch gegen das Kurzschlussrisiko abzusichern. Ein Filer muss daher zunächst entsprechend gehärtet werden. Für NetApp Filer gibt es beispielsweise einen Report, der die Umsetzung der Anforderungen des Payment Card Industry (PCI) Data Security Standard (DSS) für das NetApp-Betriebssystem ONTAP beschreibt[7]. Dieser Report kann neben dem oben erwähnten Grundschutzbaustein als eine Härtungsgrundlage dienen.

Bei NetApp Filern, wie sie im FlexPod eingesetzt werden, wird zur Mandantentrennung mit virtuellen Filern (vFilern) gearbeitet, die einem Mandanten exklusiv

[7]Siehe http://www.netapp.com/mx/system/pdf-reader.aspx?pdfuri=tcm:38-60687-16&m=tr-3996.pdf

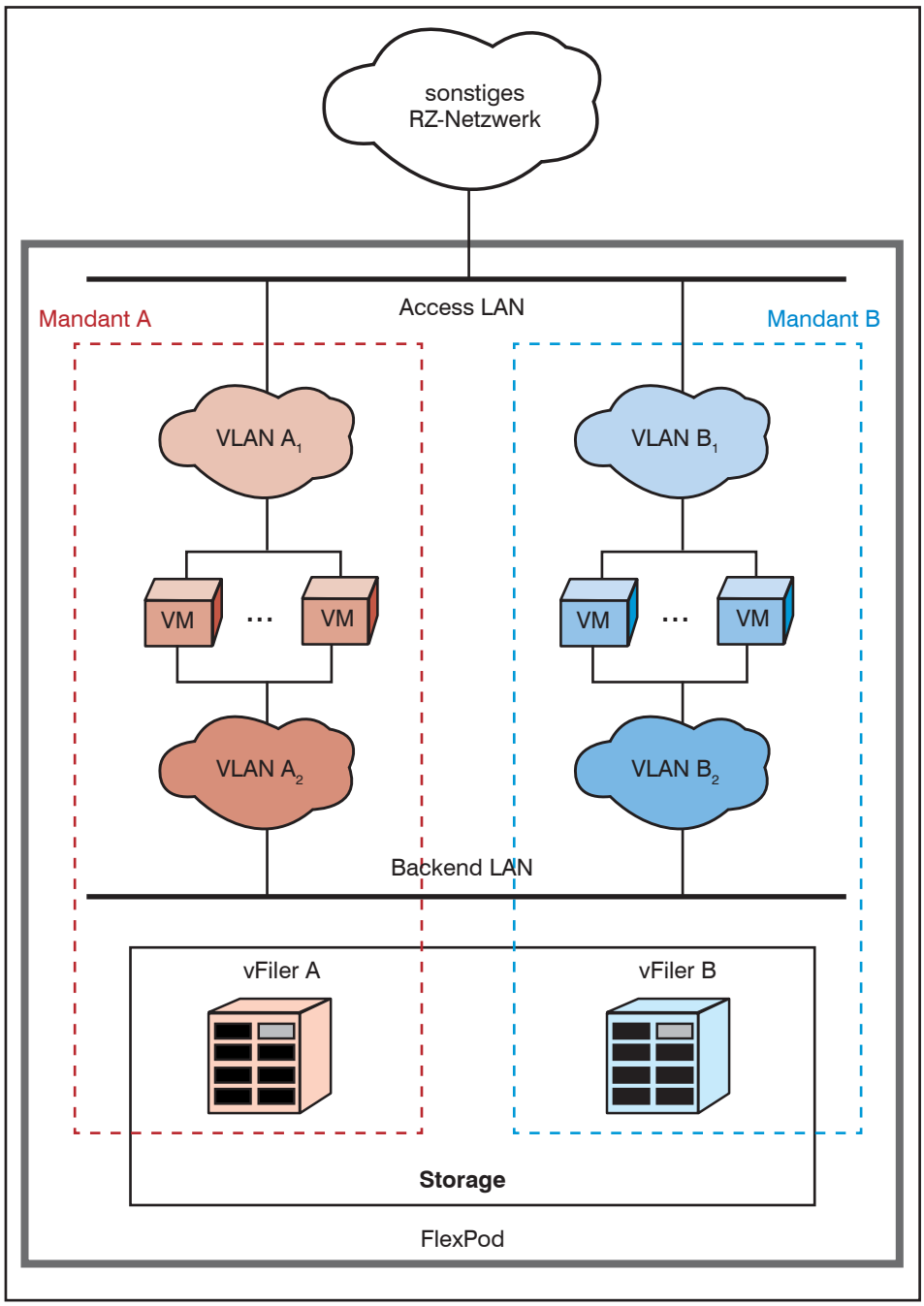


Abbildung 7: Trennung des Storage-Verkehrs

zugeordnet werden. VMs werden dabei dual-homed angebunden und erhalten ein Interface für den funktionalen Zugriff (d.h. Zugriff auf Anwendungen) und ein separates Interface für den Storage-Zugriff. Diese Interfaces werden unterschiedlichen VLANs zugeordnet. Auf diese Weise wird der Storage-Verkehr effektiv vom sonstigen Verkehr getrennt. (siehe Abbildung 7)

3.6 Übergreifende Maßnahmen Data Center in a Box

Abschließend sind Sicherheitsmaßnahmen wesentlich, welche die Gesamtlösung als Ganzes betrachten. Dies betrifft insbesondere die Kontrolle der Zusammenarbeit zwischen den Einzelkomponenten einer ViS-Lösung.

Festlegung von klar umrissenen Mandantenprofilen

Die entscheidende Grundlage ist die genaue Festlegung und Beschreibung der Mandanten. Insbesondere müssen die erlaubten Kommunikationsmöglichkeiten zwischen Mandanten und sonstigen Netzbereichen spezifiziert werden. Dabei ist es ratsam Profile für Mandanten zu spezifizieren, die für unterschiedlichen Schutzbedarf und unterschiedliche Nutzungsformen ausgelegt werden können. Ein Beispiel wäre für eine Anwendung (z.B. SAP) die Spezifikation von drei Mandanten mit einem Profil für Entwicklung und Test, einem Staging-Profil für Prelive-Systeme (d.h. Vorproduktion) und einem Profil für produktiv genutzte Systeme (siehe Abbildung 8).

Kontrolle der Mandantenkommunikation

Die Kommunikation zwischen einem Mandanten und seiner Umgebung muss kontrolliert werden. Hierzu kommen üblicherweise Firewalls zum Einsatz. Je Anforderung und eingesetzter ViS-Lösung kann hier eine entsprechend leistungsfähige Data Center Firewall oder eine Firewall, die auf Ebene von Hypervisor oder virtualisiertem Switch innerhalb der ViS-Lösung realisiert wird, verwendet werden.

Absicherung der Automatisierung

Für die Provisionierung der VMs, Systemkopien, Cloning und Deprovisionierung sind automatisierte Prozesse erforderlich. Diese sind z.B. bei FlexPod als Shell Scripts realisiert, die über den NetApp Workflow Manager bzw. NetApp Workflow Automator erstellt und bearbeitet werden können.

Die Scripts werden bei FlexPod über eine normale Shell ausgeführt. Über gruppenspezifische Ausführungsberechtigungen kann sichergestellt werden, dass keine ungeplanten Ausführungen eines Script stattfinden.

Mitgelieferte Scripts werden z.B. bei FlexPod im CVD (Cisco Validated Design) dokumentiert. In der Praxis zeigt sich immer wieder, dass diese Scripts an die jeweiligen Anforderungen und Rahmenbedingungen des Einsatzes der Lösung angepasst werden müssen und dass teilweise auch neue Scripts erstellt werden. Eine gute Dokumentation geänderter und neuer Scripts sowie ein konsequentes Change Management und Configuration Management sind dabei entscheidend.

Zur Qualitätssicherung müssen geänderte und neue Scripts getestet werden. Hierzu kann eine entsprechende Testumgebung in einem Maintenance Tenant vorgesehen werden.

Das Trouble Shooting von Scripts erfolgt auf Shell-Niveau, d.h. letztendlich über Ausgaben in eine Log-Datei.

Absicherung des Management-VLAN gegen Fehler in der Administration

Typisch für ViS-Lösungen ist der Aufbau ei-

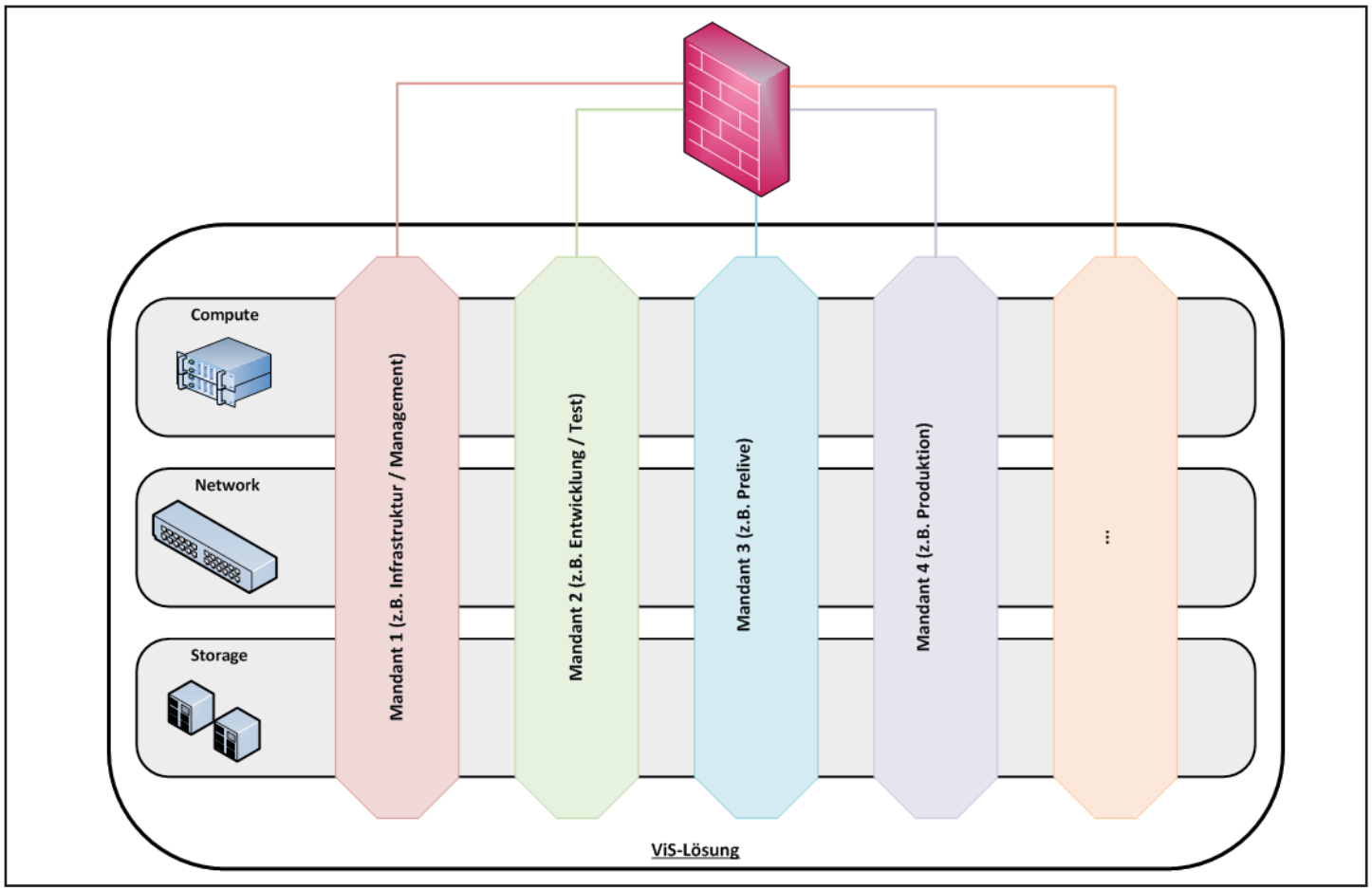


Abbildung 8: Kontrolle der Kommunikation zwischen Mandanten und Umgebung

nes Management-Mandanten bzw. eines Management-VLANs zur Trennung administrativer und funktionaler Kommunikation. Eine Gefährdung besteht nun grundsätzlich in einem unberechtigten Zugriff auf das Management-VLAN. Dieser kann beispielsweise durch die versehentliche Zuweisung eines falschen Port-Profils zu einem Gastsystem ermöglicht werden, sodass die entsprechende VM dem Management-VLAN zugeordnet wird.

Bevorzugte Maßnahme ist hier die Verwendung von MAC Address Whitelists für Management-Komponenten. Falls dies sich als nicht praktikabel erweist, kann beispielsweise bei FlexPod und Vblock eine Festlegung der maximalen Portanzahl erfolgen, sodass keine zusätzliche Maschine in das Management-VLAN provisioniert werden kann.

Regelung des Betriebs einer ViS-Lösung

Die Komponenten Server, Virtualisierungs-Host, Switches und Storage einer ViS-Lösung werden naturgemäß von unterschiedlichen Parteien (und typischerweise auch unterschiedlichen Organisationen) betrieben. Durch nicht geeignet abgestimmten Betrieb kann es einerseits zu Störungen kommen (z.B. eine nicht abgestimmte Konfigurationsänderung in einem Switch, die dazu führt, dass für einen Mandanten nicht mehr die gewünschten Kommunikationsziele erreichbar sind) und andererseits kann die Fehlersuche und die Störungsbeseitigung unnötig verlängert werden.

Daher müssen die Betriebskonzepte zielgerichtet für eine ViS-Lösung angepasst werden und zwischen den beteiligten Parteien effiziente Kommunikationswege geschaffen werden.

4. Fazit

Vertikal integrierte Systeme (ViS) statt separater Server, Storage, Netzwerk und Hypervisoren: Das scheint ein aktueller Trend zu sein. Bei diesen Systemen handelt es sich entweder um Referenz-Architekturen (z.B. FlexPod) oder um Produkte (z.B. Vblock), in denen alles miteinander kombiniert ist. Der Kunde erhält also eine Lösung, bei der er sicher sein kann, dass alle Komponenten inklusive Management-Lösung für das Gesamtpaket miteinander spielen.

Der Kunde hat also einen Vorteil von dieser Technik und zahlt wahrscheinlich gegenüber selbst zusammengestellten Komponenten einen Aufpreis. Aber insbesondere Softwarehersteller wie SAP, die bisher bereits genaue Vorgaben für die Konfiguration von Systemen gemacht haben, profitieren davon. Wenn der Kunde die Software auf einer z.B. für SAP validierten ViS-Lösung laufen lässt, kann er sicher sein, die Spezifikationen a priori zu erfüllen.

Daher werden ViS zukünftig größere Verbreitung finden und zwar überall dort, wo standardisierte Systeme unter einem Hypervisor eingesetzt werden können. Aber auch die herkömmliche Technik wird es weiter geben, denn nicht alles ist VMware, nicht alles ist X86 und nicht alle Unternehmen möchten ihre separaten Teams für Server, Storage und Netz zusammenlegen.

Auch für ViS-Lösungen gilt: Das Ganze ist mehr als die Summe seiner Einzelteile. Die Absicherung von ViS-Lösungen erfordert eine ganzheitliche Sicht, die über die Absicherung der Komponenten Server, Virtualisierungs-Host, Switches und

Storage hinausgeht und speziell das komplexe Zusammenspiel der Elemente einer ViS-Lösung berücksichtigt. Besonders kritisch ist dabei die RZ-Automatisierung zu sehen, bei der letztendlich die gesamte Konfiguration per Scripts gesteuert wird. Striktes Configuration Management und ein hohes Niveau an Qualitätssicherung sind hier essentiell.

5. Abkürzungen

ACE	Application Control Engine
ACS	Access Control Server
AD	Active Directory
AIX	Advanced Interactive Executive (IBM)
API	Application Programming Interface
BIOS	Basic Input/Output System
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BSI	Bundesamt für Sicherheit in der Informationstechnik
CM	Configuration Management
CPU	Central Processing Unit
CVD	Cisco Validated Design
DC	Data Center
DSS	Data Security Standard
ESR	Embedded Service Router
FC	Fiber Channel
FCoE	Fiber Channel over Ethernet
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IaaS	Infrastructure as a Service
ICSA	International Computer Security Association
IP	Internet Protocol
IT	Informationstechnik
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number
MAC	Media-Access-Control
NAS	Network Attached Storage
NFS	Network File System
NIC	Network Interface Card
PCI	Payment Card Industries
QoS	Quality of Service
RZ	Rechenzentrum
SaaS	Software as a Service
SAN	Storage Area Network
SEL	System Event Log
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSO	Stateful Switchover
TMT	Trusted Multi-Tenancy
UCS	Unified Computing System
UIM	Unified Infrastructure Manager
USA	United States of America
ViS	Vertikal integrierte Systeme
VRF	Virtual Routing and Forwarding
VCE	Virtual Computing Environment Company
VDI	Virtual Desktop Infrastructure
VLAN	Virtual LAN
VM	Virtual Machine
WWN	World Wide Name
XML	Extensible Markup Language

ComConsult-Study.tv

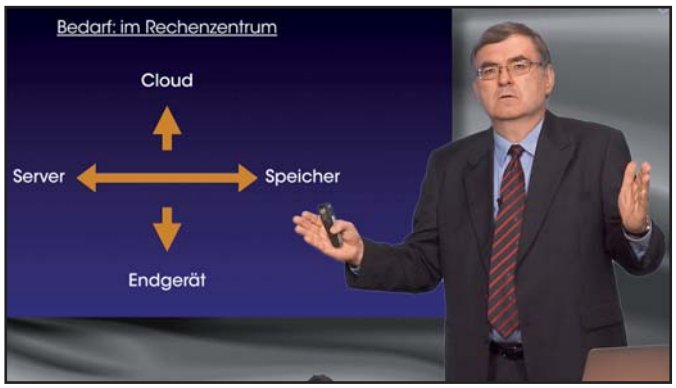
Oster-Aktion

Im April 15% auf das Jahres-Abo von ComConsult-Study.tv

Die Netzwerk Welt ist im Umbruch. Aktuell stehen Änderungen wie seit Jahren nicht mehr an. Selbst als IT-Experte verliert man leicht den Überblick und unklar ist, wo der Weg hingeht. ComConsult-Study.tv bietet deshalb eine Reihe Videos mit Trend-Analysen und Technikvergleichen, in denen Top-Experten den aktuellen Stand der Technik vorstellen und bewerten.

Herausragend in diesem Angebot ist das Video „Cisco unter Druck? Die Zukunft der Netzwerk-Branche“, in dem Dr. Suppan analysiert, wie und warum sich Computer-Netze in Zukunft ändern werden.

Dieses Video ist exklusiv für Abonnenten von ComConsult Study.tv und Teilnehmer des ComConsult Netzwerkforums 2014. Es kann nicht einzeln gekauft werden.



Cisco unter Druck? Die Zukunft der Netzwerk-Branche

Referent: **Dr. Jürgen Suppan**
Zeit: 01:10:48

Die Netzwerk-Branche ist unter Druck. Cisco als Marktführer ist ein Spiegel der Branche. Dr. Jürgen Suppan analysiert wie sich die Computer-Netze verändern werden.

Microsoft Surface Pro 2: besser als das iPad Air für Unternehmen?
Referent: **Dr. Jürgen Suppan**
Zeit: 00:52:12

Mit dem Surface Pro 2 bringt Microsoft nun zum ersten Mal ein Gerät, das hohe Erwartungen weckt. Ist hier zum ersten Mal eine Integration aus Tablet und Windows gelungen? Hat damit das iPad Air für Unternehmen an Bedeutung verloren?

Statt € 398,-- netto zahlen Sie nur € 338,-- netto

Zögern Sie nicht, sich das Abonnement im April mit 15% zu sichern. Auch die Nutzungslizenzen für mehrere User oder über mehrere Jahre sind reduziert. Zögern Sie nicht uns anzusprechen. Gerne senden wir Ihnen ein persönliches Angebot zu.

Weitere Details finden Sie auf unserer Homepage unter www.comconsult-study.tv

Aktuelles Seminar

Intensivtag: Tod des Tischtelefons und danach Cloud-Lösungen?

27.05.14 in Bonn

Die ComConsult Akademie veranstaltet am 27.05.2014 ihren "Intensivtag: Tod des Tischtelefons und danach Cloud-Lösungen?" in Bonn.

Die Technologie für TK- und UC-Lösungen ist weiterhin in einem sehr schnellen Wandel begriffen. Gerade die zukünftige Rolle des Telefons und seine Umsetzung wird dabei von neuen Technologien immer mehr in Frage gestellt:

- Welche Zukunft hat das Telefon: Müssen wir umdenken? Was steht in Zukunft auf unseren Schreibtischen?
- Endgeräte in der Diskussion: Tischtelefon oder Softclient?
- Welchen Einfluss haben neue Webtechnologien wie WebRTC auf das Endgerät der Zukunft?
- TK oder UC: was ist besser und was bedeutet das in der Praxis?
- Hosted PBX: liefert die Cloud die Basis für die TK-/UC-Lösung der Zukunft?

Erste Prototypen der Hersteller in den Labors deuten auf einen dramatischen Wandel in der Endgeräte-Landschaft hin. Das bedeutet nicht, dass wir in Zukunft keine Telefone mehr haben werden, aber sie werden völlig anders aussehen und auf einer stark veränderten Basis aufgebaut sein. Mit der Einführung von WebRTC

wird der Browser zum universellen TK-Client, und das mit einer herausragenden Qualität.

Auch die durchaus umstrittene Cloud nimmt an Bedeutung gerade für UC-Lösungen zu. Die Weiterentwicklung der Technologie bei den großen Cloud-Providern verschiebt die wirtschaftlichen Potenziale deutlich. Ohne Frage können heute nach vielen Jahren der Diskussion Hosted PBX-Lösungen zu Preisen umgesetzt werden, die weit unter den internen Kosten der Unternehmen liegen. Aber dies ist verbunden mit einer Vielzahl von Fragen, von der Abhängigkeit über die Qualität bis hin zur Gestaltbarkeit der Lösung. Aber Unternehmen haben durchaus die Chance, zu ähnlichen Technologien zu greifen wie sie auf der Provider-Seite eingesetzt werden und ihre Kosten deutlich zu senken.

Es ist an der Zeit, Telefonie und UC-Lösungen neu zu positionieren und ein Maximum aus den neuen Möglichkeiten herauszuholen.

Hier setzt unser Intensiv-Tag "Tod des Tischtelefons und danach Cloud-Lösungen?" an. Wir analysieren und diskutieren für Sie die neuesten Entwicklungen und stellen uns den Themen:

- Die Zukunft des Tischtelefons
- Wie verändert WebRTC die Kommunikation?
- Enterprise Lösungen für TK und UC
- Hosted PBX: Motivation und Angebote
- Was kommt nach S2M: SIP Trunking und Alternativen als Pushfaktor von Cloud Lösungen
- Kontroverse Diskussion: Vor- und Nachteile von Enterprise und Cloud Lösungen

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Intensivtag: Tod des Tischtelefons und danach Cloud-Lösungen?

Ich buche das Seminar
Intensivtag: Tod des Tischtelefons und danach Cloud-Lösungen?

☐ am 27.05.14 in Bonn
zum Preis € 990,-- netto

Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 14

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Zweitthema

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus?

Teil 3

Fortsetzung von Seite 1

Dipl.-Inform. Petra Borowka-Gatzweiler leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Loop-Unterbindung erfolgt jedoch nicht mit Spanning Tree, sondern der vSwitch weiß per interner Software, welche MAC Adresse wo angebunden ist und wie Loops vermieden werden (siehe hierzu auch IEEE Standard 802.1bg). Link Aggregierung, Teaming oder Failover können jedoch wie bei phyNICs konfiguriert werden.

Ein Host-Administrator kann mit den hostinternen Konfigurationsmöglichkeiten soweit gehen, dass er einen hostinternen virtuellen Switch, an den alle VMs angeschaltet sind, mittels virtuellem Firewall weitestgehend von der Außenkommunikation abschirmt und die Konnektivität nach außen durch einen dem Firewall nachgeschalteten zweiten vSwitch realisiert wird wie in Abbildung 7.1 dargestellt.

Ähnliches gilt für die Konfiguration virtueller Router. Alle vSwitches innerhalb eines Hosts können gegenüber der physischen Netzwerk-Welt komplett durch virtuelle Router abgekoppelt werden, so dass alle Layer-2 Prozesse innerhalb des Hostsystems terminiert werden. Zwischen den vSwitches und vRoutern lassen sich vom Administrator analog zu physischen Netzkomponenten im Prinzip beliebige Verbindungen konfigurieren. Ein Beispiel zeigt Abbildung 7.2. Die Technik virtualisierter Load Balancer, Router und Firewalls ist noch jung, daher ist hinsichtlich der möglichen Funktionalität von Einschränkungen und gegebenenfalls Kinderkrankheiten auszugehen. Tatsächlich lassen sich aber mit virtuellen Netzkomponenten innerhalb eines Hosts komplette virtuelle Subnetzwerke bilden, auf die der Netzbetreiber vorab keinen oder nur bedingten Zugriff hat. Dieser erfolgt, soweit er gegeben ist, immer über spezielle Managementmodule oder Produkte zur Integration von physischem Netzwerk und Virtualisierungs-Umgebung, die meistens der Netzwerk-Hersteller entwickelt und anbietet, da sich die Virtualisierungs-Hersteller wenig um die Integration ins physische Netzwerk kümmern.

Im Prinzip gelten für virtuelle Netzkomponenten die gleichen Design-Prinzipien wie für physiche Netzkomponenten, insbesondere hinsichtlich Überbuchung und Failover.

8. Wo kommt welches Failover-Verfahren zum Einsatz?

Im Rahmen des Netzwerk-Designs ist in jedem Fall auch die Frage zu beantworten, wo welche automatischen Schaltverfahren zum Einsatz kommen sollen, soweit keine individuelle Netzwerk-steuerung mit SDN angestrebt ist – was jedoch in diesem praxis-orientierten Beitrag mangels breiter Verfügbarkeit und Erfahrungswerte außer Acht gelassen wird.

Zur Auswahl stehen aktuell:

- Link Aggregierung
- Multi-Chassis Link Aggregierung
- Layer-2 Multipath (SPBM, TRILL)
- Spanning Tree
- FC FSPF (standardisiert im SAN / FC Umfeld)
- Proprietäre Fabric Verfahren (FabricPath, VCS, QFabric und andere)
- OSPF Routing
- MPLS

FSPF ist standardisiert auf den Fibre Channel SAN-Bereich beschränkt, proprietäre Verfahren haben ihre Probleme im Trouble Shooting und im Migrationsfall, Spanning Tree ist tatsächlich in die Jahre gekommen und auch in der RST Variante inzwischen vielfach nicht mehr sehr geliebt, wenn auch wegen ihrer Bekanntheit und Etabliertheit immer noch im Einsatz.

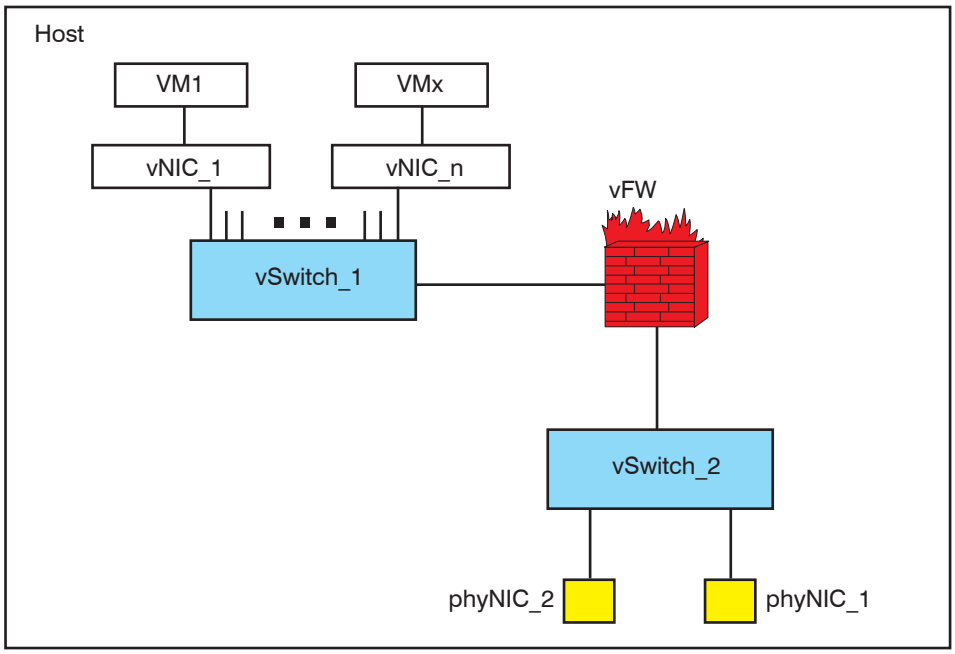


Abbildung 7.1: Hostinterne vSwitch und vFW Konfiguration

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 3

Kümmern wir uns im Nachgang um die moderneren und zukünftig anstehenden Layer-2 Verfahren wie Link Aggregierung, Multi-Chassis Link Aggregierung, Layer-2 Multipath sowie OSPF und MPLS. Aufgrund der Einschränkung auf zwei parallel verbundene Systeme hat Link Aggregierung im Data Center stark an Bedeutung verloren. Hier kommen überwiegend lastverteilte Verfahren zum Einsatz, die Redundanz über mehrere Systeme ermöglichen. Im Campus und Gebäudebereich sind LAGs etabliert und gut einsetzbar.

Multi-Chassis Link Aggregierung ist unter der Bezeichnung DRNI (Distributed Resilient Network Interconnect, IEEE 802.1AX Maintenance Release) die Weiterentwicklung der Link Aggregierung, auch mit proprietären Vorläufern wie VSS, MEC, Bonding, IRF, SMLT und anderen. Hier gibt es wenige Einschränkungen in der Skalierbarkeit, das Verfahren ist im Prinzig beliebig kaskadierbar und in allen Layer-2 Bereichen gleichermaßen einsetzbar, wie seinerzeit der Spanning Tree.

Layer-2 Multipath ist grundsätzlich ein Layer-2 Verfahren, leistet also nicht die Verbindung verschiedener IP Subnetze / verschiedener VLANs. Da aber die Konfigurationsflexibilität sehr hoch und die Lastverteilung sehr gut ist, kann der Netzbetreiber zum Beispiel darüber nachdenken, das Campus Netzwerk anstelle von lauter OSPF Transit Links zu einem gemeinsamen Backbone-Subnetz mit Layer-2 Multipath zu konfigurieren und somit viele Transit-Netze einsparen. Daher gibt es für Layer-2 Multipath wie auch MC-LAG in allen Netzbereichen sinnvolle Einsatzszenarien. Zudem erlaubt Layer-2 Multipath die transparente und lastverteilte Verbindung gleicher VLANs und überlappender VLAN-IDs verschiedener Mandanten über einen Backbone hinweg. In diesem Sinn kann Layer-2 Multipath im Campus Backbone ein Ersatz von MPLS werden, das sich ja gerade zur Handhabung vieler und auch überlappender VLANs in den letzten Jahren in großen Campus-Netzwerken etabliert hat.

OSPF als Layer-3 Verfahren kommt innerhalb von Gebäuden überschaubarer Größe eher nicht zum Einsatz, ist aber im Gebäude-Campus-Übergang und für den Campus sehr gut geeignet. Da im RZ für HA-Konzepte vielfach Layer-2 Verbindungen erforderlich sind, ist OSPF als Layer-3 Verfahren nur bedingt und übergreifend zur Kopplung verschiedener Subnetze einsetzbar, und auch nur, wenn im RZ-Bereich eine einfache geroutete Kopplung als zulässig betrachtet wird und keine höherwertigen Schutzkonzepte implementiert werden.

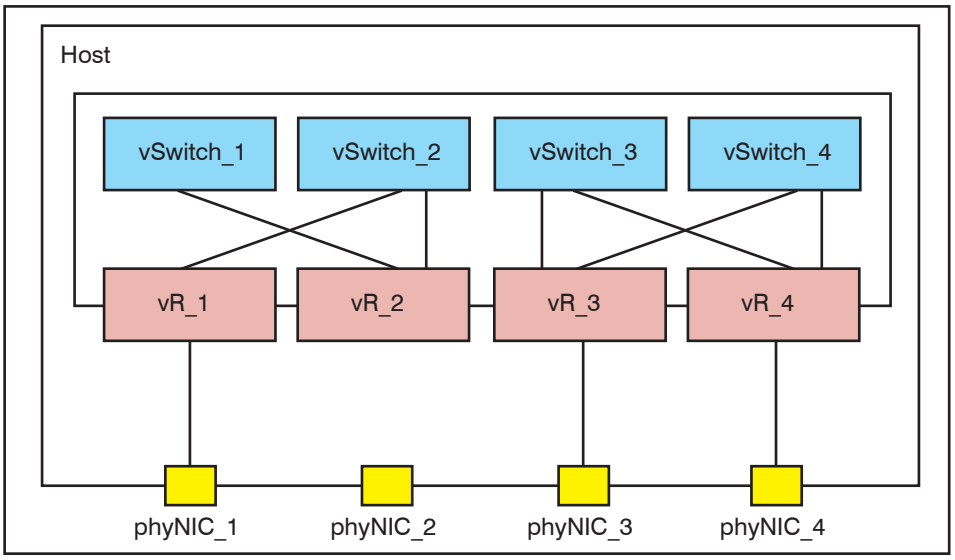


Abbildung 7.2: Hostinterne vSwitch und vFW Konfiguration

Grundsätzlich gilt: Je einheitlicher die eingesetzten Verfahren in Accees, Campus und Data Center Bereich sind, umso übersichtlicher gestaltet sich der Netzbetrieb.

Abbildung 8.1 zeigt eine Übersicht über Redundanz- und Lastverteilungs-Verfahren und ihre jeweiligen Einsatzbereiche.

Abkürzungen, Links, Literatur

AP	Access Point
DRNI	Distributed Resilient Network Interconnect
EAPS	Ethernet Automated Protection Switching (Extreme Networks, IETF RFC 3619)
ECMP	Equal Cost MultiPath
EoR	End-of-Row
FC	Fibre Channel
fdx	full duplex
FDDI	Fiber Distributed Data Interface
FSPF	Fabric Shortest Path First
HiPER Ring	High-Performance Redundancy (HiPER) ring protocol (Hirschmann EP 2343857 A1)
IRF	Intelligent Resilient Framework
LAG	Link Aggregation Group
LWL	Lichtwellenleiter
MC-LAG	Multi-Chassis LAG
MEC	Multi-Chassis EtherChannel (Cisco)
MLAG	Multiswitch LAG (Extreme)
MPLS	Multi Protocol Label Switching
MPP	Massively Parallel Processing
MRP	Media Redundancy Protocol
MRP	Metro Ring Protocol
NIC	Network Interface Card (Coupler)
OM	Optical Multimode
OSPF	Open Shortest Path First
phyNIC	physische NIC
PoE	Power over Ethernet
QF	QFabric (Juniper)
RFC	Request For Comment; TCP/IP Standard-Dokument
RZ	Rechenzentrum
SAN	Storage Area Network
SPB	Shortest Path Bridging
SPBM	Shortest Path Bridging MAC
SMLT	Split Multilink-Trunking
SPBM	Shortest Path Bridging MAC
SPBV	Shortest Path Bridging VID
SPoF	Single Point of Failure
ToR	Top-of-Rack
TRILL	TRansparent Interconnection of Lots of Links
UC	Unified Communications
VCS	Virtual Cluster Switching (Brocade)
vFW	virtuelle Firewall
vLB	virtueller Load Balancer
VoIP	Voice over IP
vR	virtueller Router
vSw	virtueller Switch

Failover Verfahren	RZ	Campus	Gebäude
Link Aggregierug	(✓)	✓	✓
Multi-Chassis LAG	✓	✓	✓
Layer-2 Mulipath	✓	✓	✓
FC FSPF	(✓)	✗	✗
Rapid Spanning Tree	✗	✗	(✓)
OSPF	(✓)	✓	(✓)/✗
MPLS	✗	✓	✗

Abbildung 8.1: Übersicht über die Einsetzbarkeit von Stern- Ring- und vermaschten Designs

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Lokale Netze für Einsteiger - Intensiv Seminar, 05.05. - 09.05.14

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.490,-- netto

Aufbau und Management von Internet-DMZ und internen Sicherheitszonen, 05.05. - 06.05.14 in Bonn

Die IT-Sicherheit für die Internet DMZ und internen Sicherheitszonen wird in diesem Seminar von Experten aus der Praxis analysiert. Verschiedene IT-Architekturen und Konzepte werden analysiert und auf ihre Praxistauglichkeit untersucht. Die Umsetzung anhand konkrete Projektbeispiele runden die Schulung ab.

Preis: € 1.590,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 05.05. - 07.05.14 in Bonn

Dieses Seminar vermittelt alle notwendigen Projektschritte die zu einer erfolgreichen Umsetzung von VoIP Projekten benötigt werden. Diese erstrecken sich über die Einsatz- und Migrations-Szenarien, die einsetzbaren Basis-Technologien und Komponenten und die erweiterten TK-Anwendungen wie IVR, UM oder UC. Es werden Bewertungskriterien für eine TK-Lösung und eine Übersicht über den bestehenden TK-Markt mit allen etablierter Hersteller vorgestellt.

Preis: € 1.890,-- netto

Ausschreibungen im Informations- und Kommunikationsbereich, 12.05.14 in Bonn

Dieses 1-tägige Seminar bietet einen praxisnahen Leitfaden für öffentliche Auftraggeber, die in ihren ITK-Vergabeverfahren unter Einhaltung aller gesetzlichen Auflagen das optimale Ausschreibungsergebnis erreichen wollen. Auch die Vertreter von Unternehmen lernen hier für ihre Ausschreibeungen die Rechts- und Investitionssicherheit zu verbessern und ein optimales Angebotsverhalten zu erreichen.

Preis: € 990,-- netto

Wireless LAN professionell , 12.05. - 14.05.14 in Bonn

Lernen Sie in diesem Seminar wie Sie eine WLAN-Lösung zukunftsorientiert und investitionssicher für die verschiedensten Endgerätetypen und Dichten aufbauen. Lernen Sie wie sie Verfügbarkeit und Bandbreite optimieren. Verbessern Sie Ihr WLAN mit den verschiedensten Struktur-Elementen vom Access-Point bis zum WLAN-Controller. Erfahren Sie worin sich Produkte und Technologien führender Anbieter unterscheiden. Berücksichtigen Sie die neusten Entwicklungen zur Gestaltung einer WLAN-Lösung, die langfristig tragfähig und wirtschaftlich ist. Lernen Sie Vor- und Nachteile aller aktuellen Technologien kennen und vermeiden Sie Planungs-Fehler.

Preis: € 1.890,-- netto

WAN: Konzept, Planung und Ausschreibung, 19.05. - 20.05.14 in Bonn

Seminar über die erfolgreiche Konzeption, Planung und Betrieb von WAN-Netzwerken. Lernen Sie wie Sie mit modernsten Technologien und erprobten Architekturen wirtschaftliche, verfügbare und leistungsfähige WAN-Lösungen aufbauen können. Erfahren Sie wie Sie sinnvoll SLAs für die Praxis aufsetzen können, die auch im Tagesbetrieb standhalten. Mit vielen Tipps und Tricks aus der Praxis.

Preis: € 1.590,-- netto

Trouble Shooting in vernetzten Infrastrukturen, 20.05. - 23.05.14 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator-Software kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.290,-- netto

Rechenzentrumsdesign - Technologien neuester Stand, 26.05. - 28.05.14 in Bonn

Dieses Seminar analysiert die neuesten Technologie-Trends im Rechenzentrum. Sie lernen von der Verkabelung über die Stromversorgung, die Klimatisierung und den Schrankaufbau, wie ein ausfallsicheres und energieeffizientes Rechenzentrum heute strukturiert wird. Mechanismen für Redundanz im Netzwerk, Lastverteilung und Standort-übergreifende Hochverfügbarkeit werden diskutiert und es wird untersucht wie diese mit dem fortwährenden Trend zur Virtualisierung zusammenspielen. Abschließend werden aktuelle Speichersysteme, deren Anbindung über die am Markt verfügbaren Übertragungsprotokolle sowie Aspekte zur Datensicherung und Disaster Recovery diskutiert.

Preis: € 1.890,-- netto

Recht und Datenschutz bei Einführung von Voice over IP, 26.05. - 27.05.14 in Bonn

Ziel der Schulung ist es, den Teilnehmern einen Überblick über die aktuelle Situation im Bereich des Datenschutzes im Kommunikationsumfeld zu verschaffen. Datenschutz und Datensicherheit werden zunehmend wichtiger im Umgang mit Kunden und Mitarbeitern. Gerade mit der Einführung von IP basierten Lösungen in den Bereichen Telefonie oder Contact Center, stellen sich neue Herausforderungen in Bezug auf personenbezogene Informationen. Um Ihnen eine Überblick über den rechtlichen Rahmen zu geben beschäftigt sich dieses Seminar u.a. mit Fragen zur Abhörsicherheit, Vorratsdatenspeicherung, Datenverlust und den dazugehörigen Aspekten. Weitere Schwerpunkte bilden die etwaigen Vorgaben seitens der Bundesnetzagentur oder auch von Betriebsvereinbarungen, die es zu beachten gilt.

Preis: € 1.590,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
05.05. - 09.05.14 in Aachen
08.09. - 12.09.14 in Aachen
17.11. - 21.11.14 in Aachen

TCP/IP-Netze erfolgreich betreiben
02.06. - 04.06.14 in Aachen
20.10. - 22.10.14 in Aachen

Internetworking
23.06. - 27.06.14 in Aachen
03.11. - 07.11.14 in Aachen

Paketpreis für zwei 5-tägige und ein 3-tägiges Intensiv-Seminar € 6.180,-- netto (Einzelpreise: € 2.490,-- netto bzw. 1.890,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
20.05. - 23.05.14 in Aachen
28.10. - 31.10.14 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
24.06. - 27.06.14 in Aachen
18.11. - 21.11.14 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,-- netto
(Seminar-Einzelpreis € 2.290,-- netto , mit Prüfung € 2.470,-- netto)

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
05.05. - 07.05.14 in Bonn
29.09. - 01.10.14 in Stuttgart
17.11. - 19.11.14 in Bonn

Basis-Technologie der IP-Telefonie
02.06. - 04.06.14 in Düsseldorf
20.10. - 22.10.14 in Berlin

Umfassende Absicherung von Voice over IP und Unified Communications
30.06. - 01.07.14 in Bonn
03.11. - 04.11.14 in Bonn

Session Initiation Protocol

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
15.09. - 16.09.14 in Düsseldorf

Wir empfehlen die Teilnahme an diesem Seminar **"IP-Wissen für TK-Mitarbeiter"** all jenen, die die Prüfung zum ComConsult Certified Voice Engineer anstreben, ganz besonders aber den Teilnehmern, die bisher wenig bis kein Netzwerk Know How, insbesondere TCP/IP, DNS, SIP usw., vorweisen können.

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 4.840,-- netto statt € 5.370,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

Impressum

Verlag:
ComConsult Research Ltd.
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie