

OBECO GMBH

IT Konzept

Fa. Mittelstand

Joachim Berger



Impressum:

Obeco GmbH
Arenberger Str. 230a
56077 Koblenz

Telefon : 0261-9634466-0

Fax: 0261-9634466-1

Mail: info@obeco.de

Web: www.obeco.de

Geschäftsführer: Joachim Berger, Amtsgericht Koblenz, HRB 23806

Inhaltlich verantwortlich gemäß § 55 Absatz 2 RStV: Joachim Berger (Anschrift wie oben)

Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz: DE159643101

Kto.-Nr. 650005, BLZ 505 300 05, Cronbank Dreieich

Stand: 28.10.2008 / August 2016

© Obeco GmbH alle Rechte vorbehalten

Inhaltsverzeichnis

Einführung.....	4
Vorgehensweise	4
Istanalyse / Sollkonzept.....	5
Logischer Entwurf	5
Virtuelles Design	5
Physikalisches Design	6
Sicherungskonzeption	7
Migrationskonzept (was).....	7
Rolloutkonzept (wie).....	7
Betriebskonzept.....	8
Aufwandsabschätzung	8
Konzeption.....	9
Realisation	10
Offene Punkte.....	11

Einführung

Fa. Fa. Mittelstand verfügt über ein gewachsenes IT-Umfeld mit heterogener System-Landschaft. Diese Architektur hat heute die folgenden bekannten Nachteile:

- Geringe Akzeptanz beim Endanwender
- Hohes Pflegeaufkommen im Betrieb
- Fehlende Flexibilität im Umfeld der Filialintegration

Es wurde daher beschlossen auf ein System zu migrieren, das den ca. 200 internen Anwendern in der Zentrale und ca. 300 externen Benutzern in ca. 5 Filialen eine zukunftsfähige Plattform bietet:

- Bessere bzw. hohe Akzeptanz beim Endanwender
- Konsolidierte Systemstruktur
- Reduktion von Komplexität (Abbau der Hersteller- und Programmvielfalt)
- Kontrollierbarkeit und effektivem Operating
- Betriebskonzept für Rollout, Migration und Betrieb der Filialen

Hierbei gehen wir davon aus, dass der Neubetrieb zunächst unabhängig vom Istbetrieb installiert wird. Zug um Zug werden dann die vorhandenen Funktionen in die neue Systemlandschaft migriert.

Vorgehensweise

Für ein Projekt dieser Größe und Anforderungen empfehlen wir folgende Vorgehensweise



die wir im Folgenden beschreiben.

Istanalyse / Sollkonzept

Die Istanalyse beschreibt den derzeitigen Stand Ihres IT Systems. Sie ist die funktionale Sicht auf Tätigkeiten, die der Anwender für seine Arbeit benötigt. Das Mengengerüst für Zentrale und Filialen listet alle Funktionen tabellarisch auf und umfasst z.B. folgende Daten:

- Funktion (z.B. Mailverkehr)
- Anzahl der Benutzer
- Speicherbedarf
- Verfügbarkeit

Die Istanalyse wird für alle beteiligten Betriebsstätten durchgeführt.

Die interne Verkehrsanalyse zwischen den Filialen untersucht welche Dateninhalte und Datenmengen zwischen Filialen verkehren und wo die jeweils führenden Systeme liegen.

Die externe Verkehrsanalyse verfolgt welche Dateninhalte und Datenmengen externe Einheiten (Kunden im Internetshop, Roadwarrior, Support, ...) mit internen Abteilungen / Filialen austauschen.

Aus den Mengengerüsten und den Verkehrsanalysen leiten sich die Vorgaben (Sollkonzept) für den logischen Entwurf ab.

Logischer Entwurf

Der logische Entwurf setzt die funktionalen Anforderungen in ein logisches IT-Konzept um. Dieses regelt die für den Systembetrieb erforderlichen Voraussetzungen (z.B. Aktive Directory) sowie die Umsetzung in die jeweilige Applikation (z.B. Exchange) und deren Gliederung (zentral: dezentral).

Beispiel:

Das Sollkonzept fordert: „in den Filialen ist eine unabhängige lokale Administration erforderlich“. Diese wird im logischen Entwurf des Berechtigungskonzeptes umgesetzt in eine Domänenstruktur, in dem die Niederlassungen durch eigene Subdomains abgebildet werden.

Virtuelles Design

Das virtuelle Design nimmt die für die jeweiligen Filialen erforderlichen Dienste und bündelt sie unter den Vorgaben von

- Kompatibilität (was passt zueinander)
- Kapazität (wie viel brauche ich davon)
- Performanz (Antwortzeiten)
- Verfügbarkeit (Aktualität)

zu einem im Betrieb koexistenzfähigen Paket.

Beispiel:

Der logische Entwurf fordert, dass in einer Filiale ein lokaler Virenschutz und ein WSUS-Server (Updateservice von Microsoft) vorhanden sein müssen. Im virtuellen Design wird nach Analyse des Lastaufkommens und nach guten Erfahrungen in anderen Projekten beschlossen beide Dienste in einem virtuellen Server abzubilden.

Hieraus entstehen die virtuellen Server, die im physikalischen Design auf die jeweilige Hardware abgebildet werden.

Physikalisches Design

Das physikalische Design regelt die Umsetzung des einzelnen virtuellen Servers in ihre jeweilige Hardware.

Bisher führte dieser Schritt auf Grund mangelnder Alternativen dazu, dass die virtuellen Server jeweils 1:1 auf einem physikalischen Server abgebildet wurden. 2 Domainkontroller waren daher immer 2 physikalische Maschinen.

Mit den heutigen Möglichkeiten der Virtualisierung (z.B. Intel Modular Server und Microsoft Hypervisor) ist diese Abhängigkeit aufgelöst und ermöglicht es der IT freier zu entscheiden und damit effizienter die Serverhardware zu planen und zu nutzen.

Mit diesem Konzept lassen sich unter einer Hardware alle erforderlichen virtuellen Strukturen vorteilhaft abbilden.

Szenario A:

Zum Rollout in einer neuen Filiale musste mit der bisherigen Technologie der Server entweder lokal vorinstalliert und danach verschickt werden, oder ein Servicetechniker in der Filiale musste Installation und Konfiguration durchführen. Besonders bei Domaincontrollern sind hier besondere Sicherungsmaßnahmen zu beachten.

Unter einer virtuellen Umgebung wird der Domainkontroller jedoch in der Zentrale komplett installiert und konfiguriert. Dann wird er als Datei zur Filiale kopiert und dort in die virtuelle Umgebung der Filiale eingebunden und gestartet.

Szenario B:

Zum Test neuer Programmversionen (Betriebssysteme, Mailserver, Servicepacks, Security-patche), für einen Integrations-, Last- oder Kompatibilitätstest was es bisher immer schwierig eine der Realität nahekommende Testumgebung zu bekommen.

Ist die IT-Landschaft virtualisiert, kann gegebenenfalls die komplette Umgebung per Snapshot dupliziert und für den Test benutzt werden.

Zudem lässt sich diese Hardware effektiv skalieren und ermöglicht es durch Einbau von zusätzlichen Boards, Speicher und Festplatten vorhandene Installationen nach Bedarf zu erweitern ohne die Managementkosten zu vergrößern.

Beispiel:

Im virtuellen Design wird z.B. für Filiale A folgendes gefordert:

- virtueller Server A für Domainkontroller und WSUS, 2 GB Ram, 40 GB Betriebssystem und 80 GB Daten
- virtueller Server B für Virenschutz und Backup Domaincontroller , 2 GB Ram, 20 GB Betriebssystem
- virtueller Server C für Exchange, 4 GB Ram, 20 GB Betriebssystem, 40 GB Daten

Diese Anforderungen werden z.B. in einem physikalischen Server unter Microsoft Hypervisor mit 16 GB Ram, 500 GB Datenspeicher Raid5 netto umgesetzt. Alle virtuellen Server arbeiten innerhalb von Computer Module 1. Der Computer Module 2 dient als Cold-Standby.

Sicherungskonzeption

Die Sicherungskonzeption stellt die erforderlichen Vorgaben für Szenarien der Verfügbarkeit, Backup und Restoreprozeduren zusammen.

Sie fasst folgende Anforderungen

- betriebsspezifische Anforderungen: Backup Betriebssystem Server 1
- anwendungsspezifischen Anforderungen: SQL-Server täglich sichern
- funktionalen Anforderungen: Systemwiederherstellung aller Komponenten im Katastrophenfall innerhalb von einem Kalendertag
- andere: Archivierungspflicht 10 Jahre

zu einem stimmigen Gesamtkonzept zusammen und macht Vorgaben für Hardware, Software und Prozeduren der Sicherungslogik.

Migrationskonzept (was)

Das Migrationskonzept beschreibt pro Filiale und für jede Funktionalität die erforderliche Zeit, Knowhow und Methodik, die die Alt-Umgebung in die Neu-Umgebung überführt.

- Benutzeraccounts migrieren
- Anwendungsdaten übernehmen
 - Fileserver
 - Mail
 - Anwendung A, Anwendung B, ...
- Hardware und Software

Rolloutkonzept (wie)

Im Rolloutkonzept werden die im Migrationskonzept beschriebenen Änderungen in einen Projektplan zusammengestellt. Er bestimmt in Abstimmung mit den Kapazitäten von Zentrale, Filialen, Personal, Budget und Verfügbarkeit der beteiligten Komponenten die Realisation der neuen IT Umgebung.

Betriebskonzept

Das Betriebskonzept beschreibt welche Tätigkeiten für die Aufrechterhaltung und Weiterentwicklung aller Komponenten erforderlich sind.

Beispiele:

- Wie wird der laufende Betrieb überwacht
- Wie wird Verfügbarkeit und Performanz gemessen
- Welche Produkte werden hierzu eingesetzt
- Wie wird der Rollout neuer Produkt, Versionen, Servicepacks, Updates durchgeführt und überwacht

Aufwandsabschätzung

Zum aktuellen Zeitpunkt sind die tatsächlichen Anforderungen noch sehr vage. Insbesondere ist heute nur unvollständig erkennbar welche Teilgewerke

- bisher unbekannt (Vollständigkeit)
- bereits vorhanden und erledigt
- nicht erforderlich
- in Eigenleistung
- als Fremdleistung

erbracht werden sollen. Geschätzt werden daher nur die jetzt erkennbaren Tätigkeiten zum heutigen Stand (Phase Vordesign).

Diese Tätigkeiten sind in der folgenden Aufwandsabschätzung aufgelistet. Geschätzt wurden die Aufwände zum Review der erstellten Konzepte in Bezug auf

- sachliche und inhaltliche Vollständigkeit
- Schlüssigkeit der dargestellten Zusammenhänge
- Sinngemäße Anwendung der Microsoft Architekturen
- Erfüllung der Zielvorgaben

Die hier angebotene Mitarbeit bei der Erstellung der Konzepte dient der Ergänzung des Knowhows beim Kunden und wurde mit einem Anteil von ca. 50% am Gesamtaufwand der jeweiligen Tätigkeit geschätzt.

Zur Bewertung der zur vollständigen Realisation erforderlichen Tätigkeiten fehlen uns heute ausreichend „harte“ Fakten.

Konzeption

		Manntage	
Istanalyse			
	Mengengerüste	3	
	Verkehrsanalyse intern	3	
	Verkehrsanalyse extern	3	
	Standortstrukturen 5 Standorte	5	14
Logischer Entwurf			
	Aktive Directory Aufbau, Gliederung, Namensräume	5	
	Berechtigungskonzept / Sprachen	2	
	Design Benutzerprofile	1	
	Exchange Aufbau und Gliederung	3	
	Fileserver	1	
	Virenschutz	1	13
Virtuelles Design			
	Domaincontroller	0,5	
	DNS	0,5	
	DHCP	1	
	Exchange Services	3	
	File Services	1	6
Physikalisches Design			
	Serverhardware	1	
	Storage	2	
	Konzeption Hypervisor	3	
	Netzwerk (logische Zugriffsstrukturen, IP-Bereiche)	2	8
Sicherungskonzeption			
	Pflichtenheft Vitaldienste	2	
	Redundanzen vor Ort	3	
	Backup-Szenarien	3	
	Restore Szenarien	3	
	Testumgebung	2	13
Migrationskonzept (was)			
	Benutzer	5	
	Exchange	3	
	G-Mail	5	
	Filesystem	3	16
Roll-Out Konzept (wie)			
	Zentrale	4	
	Filialen	4	8
Betriebskonzept			
	Zentrale	4	
	Filialen	4	8
	Summe		86

Realisation

Um auch den Realisationsaufwand kalkulieren zu können, haben wir im Folgenden Standardtätigkeiten und deren Aufwände aufgelistet.

Die Schätzungen basieren auf der Annahme, dass alle Schritte bis inklusive physikalischem Design erfolgreich durchgeführt wurden und auf Basis von Microsoft-Komponenten innerhalb einer Hypervisor-Visualisierungsstruktur realisiert werden.

Zentrale	Manntage	
Installation Betriebssystem, Hypervisor	1,0	
Installation Betriebssystem, Domainkontroller Fa. Mittelstand, BDC	1,0	
Installation Betriebssystem, Domainkontroller Deutschland, BDC	0,5	
Installation Betriebssystem, Exchange	1,5	
Installation Virenschutz	1,5	
Installation Fileserver	0,5	
Installation Dienste (DNS, DHCP, WSUS)	0,5	
Betriebstest Zentrale	1,0	
Migration Benutzer-Accounts	3,0	
Migration G-Mail	5,0	
Migration Exchange	3,0	
Migration Benutzerdaten	3,0	
Abschließende Dokumentation und Übergabe	2,0	
		23,5
 pro Filiale		
Installation Betriebssystem, Hypervisor	1,0	
Installation Betriebssystem, Domainkontroller	0,5	
Installation Betriebssystem, Backup-Dc	0,5	
Installation Betriebssystem, Exchange	1,0	
Installation Virenschutz	0,5	
Installation Fileserver	0,5	
Installation Dienste (DNS, DHCP, WSUS)	0,5	
Betriebstest Filiale	1,0	
Betriebstest Kommunikation Zentrale : Filiale	2,0	
Migration Mail	1,5	
Migration Benutzer-Accounts	1,5	
Migration Benutzerdaten	2,0	
Abschließende Dokumentation und Übergabe	1,0	
		13,5
 Gesamtaufwand Zentrale + 5 Filialen		91

Offene Punkte

Um den Gesamtumfang zu komplementieren fehlen uns weitere Details zu diesen Themen

- Notebooks: Mengengerüst, Datensicherheit, Anbindung, Funktionen
- Funktionalität PC : Thinclient / Terminalserver
- MS Office: Verteilung von Anwendungen
- Ausfallrechenzentrum / Notkonzept / Klima / Stromversorgung
- Anbindung Internet: Mail-Empfang, Mailversand, Webzugang, OWA, OMA, ..Shop
- Anforderungen Virenschutz in einem multinationalen, dezentral organisierten Umfeld
- Datenschutz und Datensicherheit: Datenschutzbeauftragter
- Zeiterfassung
- BDE / MDE
- SAP
- Abgrenzung technische : betriebswirtschaftliche IT
- Archivierung (SAP, Exchange,)