GWDG-Bericht Nr. 75

Thomas Baumann, Dieter Ruder,
Bertram Smolny (Hrsg.)

25. DV-Treffen der Max-Planck-Institute

18. - 20. November 2008 in Göttingen

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Thomas Baumann, Dieter Ruder,
Bertram Smolny (Hrsg.)

25. DV-Treffen der Max-Planck-Institute

18. - 20. November 2008
in Göttingen

Thomas Baumann, Dieter Ruder,
Bertram Smolny (Hrsg.)

25. DV-Treffen der Max-Planck-Institute

18. - 20. November 2008
in Göttingen

GWDG-Bericht Nr. 75
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg 11
D-37077 Göttingen
Telefon: 0551 201-1510
Telefax: 0551 201-2150
E-Mail: gwdg@gwdg.de

Satz: Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Druck: Goltze Druck, Göttingen

ISSN 0176-2516

Inhalt

Vorwort

Im Jahr 1984 initiierten einige engagierte DV-Fachleute in der Max-Planck-Gesellschaft ein Treffen für den regelmäßigen Informationsaustausch zwischen den DV-Mitarbeitern der MPG unter dem Namen „DV-Nutzertreffen“. Ihre Anregung traf ins Schwarze. Was als überschaubare Zusammenkunft begann, ist längst zu einer festen Größe im Max-Planck-Veranstaltungskatalog geworden, findet jährlich statt und erreicht mittlerweile knapp 200 Teilnehmer. Die DV-Mitarbeiter konnten 2008 ein kleines Jubiläum feiern. Das Treffen jährte sich zum 25. Mal und wurde vom 18. bis 20. November in der historischen Paulinerkirche in Göttingen abgehalten.

Die Agenda unter dem Motto „Diversität der Ideen 2.0: Zukunft ist … mobil?, …. grün?, … virtuell?“ bot neben einer Vielfalt an modernen Themen, die heute das Tagesgeschäft bestimmen, auch Raum für Retrospektiven und die Vergegenwärtigung einer rasanten Entwicklung in der IT. Eindrucksvoll hat sich bestätigt, dass der Bedarf an Diskussion und Erfahrungsaustausch unter Fachkollegen auch heute nicht an Aktualität eigebüßt hat und wesentlich zur Attraktivität des Treffens beiträgt.

Das 25. Treffen markiert nicht nur ein Jubiläum, sondern auch eine neue Qualität in der Kommunikation der DV-Mitarbeiter. In vielen wiederkehrenden Diskussionen der vergangenen Jahre wurde die Notwendigkeit unterstrichen, eine eigene Interessenvertretung zu gründen, welche die Belange ihrer Mitglieder artikuliert und koordiniert. Das Jubiläumstreffen bot einen würdi-

gen Rahmen für die Wahl des ersten IT-Sprecherkreises der Max-Planck-Gesellschaft als dedizierter Interessenvertretung der Mitarbeiterinnen und Mitarbeiter in der IT.

Die Aufgaben im Bereich der Datenverarbeitung nehmen an Umfang und Komplexität stetig zu. Dies zeigen auch die im vorliegenden Band enthaltenen Beiträge aus der Praxis einiger DV-Abteilungen der Max-Planck-Gesellschaft, die natürlich nur einen kleinen Ausschnitt aus dem breiten Themenspektrum des DV-Alltags an einem modernen Forschungsinstitut abdecken können.

Auf der Begleit-CD im Anhang finden sich weitere Informationen, die im Buch nicht berücksichtigt werden konnten. Sie enthält eine von Theo Plesser und Peter Wittenburg – zwei Initiatoren des ersten Treffens – zusammengestellte Zeitreise „25 Jahre DV-Treffen in der MPG“ und weitere Materialien u. a. zur Postersession in der Paulinerkirche. Besonders hingewiesen sei auf die Berichte von der Gründung des IT-Sprecherkreises der MPG.

Wir danken allen Vortragenden und Teilnehmern für das gelungene Jubiläumstreffen und wünschen dem Leser eine interessante Lektüre.

Jena, 10.08.2009 Thomas Baumann, Dieter Ruder, Bertram Smolny

Storagevirtualisierung mit DataCore SANmelody

Dirk Vieregg

Max-Planck-Institut für demografische Forschung, Rostock

1. Überblick

Gegen Ende des Jahres 2007 wurde am Max-Planck-Institut für demografische Forschung Rostock (MPIDF) die Serverlandschaft mit VMware ESX virtualisiert. Damit einhergehend erfolgt der Übergang von direkt angeschlossenem Speicher auf ein Storage Area Network (SAN) mit Storagevirtualisierung. Die entsprechenden Überlegungen, der Umstellungsprozess und die gewonnenen Erfahrungen sollen Inhalt dieses Beitrags sein.

2. Ausgangssituation

Anfang 2007 betrieb die IT-Gruppe des MPIDF etwa 25 Server. Dazu gehörten neben klassischen Aufgaben eines Rechenzentrums wie File-, Print- und Mailserver auch Geräte, die im Rahmen des Institutsneubaus im Jahre 2002 angeschafft worden waren und, überwiegend auf PC-Basis, Dienste z. B. für das Management der Telefonanlage oder die Zutrittskontrolle zur Verfügung stellten. Insgesamt war für die Jahre 2007 und 2008 der Austausch von ca. 10 bis 12 veralteten Servern vorgesehen.

Damals bestand am MPIDF kein SAN. Es wurde entweder mit internen Festplatten gearbeitet oder Speichersysteme verwendet, die über Fibre Channel direkt an die entsprechenden Server angeschlossenen waren. Die Speicherauslastung des Fileservers betrug ca. 85 Prozent; der Mailserver hatte nur noch 10 Prozent freie Speicherkapazität. Unter Berücksichtigung der durchschnittlichen jährlichen Zuwachsraten war eine Erweiterung bis Ende 2007 dringend geboten.

3. Servervirtualisierung

Zur Erhöhung der Verfügbarkeit von Diensten, der besseren Auslastung von Serverhardware sowie zur Verringerung der Kosten für Energie und Klimatisierung wurde die Umstellung der zu ersetzenden Server auf eine Virtualisierungslösung geplant. Dabei sollten im ersten Schritt vorrangig gering ausgelastete Server wie Web- und Printserver, Domain Controller, Lizenz- und Proxyserver sowie die Managementserver für TK-Anlage, Zeiterfassung und Zutrittskontrolle virtualisiert werden. Eine Migration größerer Systeme wie File- und Mailserver war nach einer Einführungsphase ebenfalls beabsichtigt.

Als Virtualisierungslösung wurde VMware ESX ausgewählt. Grundlage für diese Entscheidung war vor allem die breite Installationsbasis und der dadurch mögliche Erfahrungsaustausch innerhalb der Max-Planck-Gesellschaft, die dieses Produkt im Gegensatz zu konkurrierenden Lösungen wie Microsoft Hyper-V oder Xen besaß. Durch die Module High Availability (HA) und Distributed Resource Scheduler (DRS) konnten die Forderungen nach einer hohen Verfügbarkeit sowie einer besseren Auslastung der Hardwareressourcen erfüllt werden. Zur Nutzung beider Module ist ein SAN zwingend erforderlich. Details dazu werden im Abschnitt „Verfügbarkeit“ eingehender beschrieben.

4. Storagevirtualisierung

Da die Erweiterung der zentralen Speicherkapazität ohnehin geplant war, wurde dies nun auf Basis eines SAN vorangetrieben. Nachteilig schien allerdings der Umstand, dass es mit Hilfe der Servervirtualisierung zwar möglich war, eine Auslagerung von Kapazitäten in einen anderen Brandabschnitt zu realisieren, dies für den Speicherbereich jedoch einen sehr hohen Aufwand in Gestalt von teuren Speicherclustern erforderlich machte. Im Rahmen der weiteren Marktanalyse wurden Lösungen zur Storagevirtualisierung gefunden, die sowohl eine bessere Auslastung von verfügbarer Plattenkapazität als auch eine synchrone oder asynchrone Datenspiegelung an einen zweiten Standort gestatteten.

Bei internem oder direkt angeschlossenem Speicher steht jedem Server eine bestimmte Speicherkapazität zur Verfügung. Ist diese erschöpft, so müssen neue Platten hinzugefügt werden. Dies gilt auch dann, wenn andere Server über sehr viel freie Kapazität verfügen. Da es sich um getrennte Systeme handelt, kann dieser freie Speicherplatz nicht dem Server mit Speichermangel zugewiesen werden. Es ist anzunehmen, dass in der Praxis eine Vielzahl von Servern mit überdimensionierten Platten betrieben werden und die tatsächliche Auslastung nur wenige Prozent beträgt. Es gibt jedoch auch einen Vorteil: Der Ausfall eines Speichersystems betrifft in diesem Szenario nur den einen Server, der mit diesem Speicher verbunden ist.

Bei der Storagevirtualisierung werden unterschiedliche Speichersysteme zu einer Einheit zusammengefasst. Die Speicherung der Datenblöcke erfolgt verteilt über alle Festplatten und ist für den Nutzer nicht mehr transparent. Der Ausfall eines Speichergeräts hat daher gravierende Folgen für alle angeschlossenen Server. Vorteilhaft ist jedoch die Auslastung: Die freie Kapazität aller im Gesamtsystem befindlichen Festplatten kann für alle Server genutzt werden. Je nach Betriebssystem des Servers lässt sich neuer Plattenplatz im laufenden Betrieb hinzufügen. Neue Speichergeräte können ebenfalls im laufenden Betrieb eingebunden und ihre Kapazität genutzt werden.

Zur Abdeckung unterschiedlicher Bedürfnisse an Leistungsfähigkeit und Ausfallsicherheit lassen sich Festplatten verschiedener Bauarten, z. B. SATA und SAS, zu so genannten Speicherpools zusammenführen.

5. DataCore SANmelody

Am MPIDF wurde die Software SANmelody des Herstellers DataCore für die Storagevirtualisierung ausgewählt. Weitere Produkte wie SANsymphony (ebenfalls DataCore) oder IPStor von FalconStore schienen für die geplante Lösung deutlich überdimensioniert und daher auch zu teuer.

Bei SANmelody handelt es sich um eine Inband-Lösung, d. h. Daten und Steuerinformationen werden über denselben Kanal übertragen. Es können in der Anfang 2009 verfügbaren Version maximal 32 TB Speicher pro Speicherserver (Storage Domain Server, SDS) verwaltet werden. Die Software läuft auf einem Windows Betriebssystem und erweitert die Microsoft Management Console um ein entsprechendes Plugin zur Systemverwaltung. Die Anbindung der Server an den zur Verfügung gestellten Speicher kann über iSCSI oder Fibre Channel erfolgen. Als optionale Module stehen die Funktionen Snapshot, AutoProvisioning, synchrone sowie asynchrone Datenspiegelung zur Verfügung.

Sämtlicher Speicher, der von Windows-Betriebssystemen nutzbar ist, kann mit Hilfe von SANmelody virtualisiert und Applikationsservern zugewiesen werden. Es ist unerheblich, ob es sich um interne Festplatten, direkt angeschlossenen Speicher, Geräte im SAN oder sogar USB-Geräte handelt.

Zunächst erfolgt die Zusammenfassung der Speichersysteme zu Speicherpools. Dabei sollten nur Geräte mit gleichen Eigenschaften (z. B. RAID-Level, Performance) zu einem Pool zusammengefasst werden. Am MPIDF sind dies derzeit drei Pools: SAS-Platten mit RAID-5, SAS-Platten mit RAID-1 und SATA-Platten mit RAID-5. Letztere werden ausschließlich durch den Fileserver genutzt.

In der zweiten Stufe werden so genannte Network Managed Volumes (NMV) eingerichtet. Das geschieht wie der eben erläuterte Schritt auf jedem SDS separat. Diese NMVs werden später für die synchrone Datenspiegelung benötigt und haben in der eingesetzten Version von SANmelody eine unveränderliche Größe von 2 TB.

Als letzte Aufgabe bei der Erstellung eines Speicherbereichs ist es notwendig, ein virtuelles Volume auf einem SDS zu erstellen und ein NMV zuzuweisen. Bei der Nutzung des Moduls für die synchrone Datenspiegelung können dies auch mehrere NMVs auf unterschiedlichen Speicherservern sein. Virtuelle Volumes können beliebige Kapazitäten bis maximal 2 TB besitzen. Für Anfang 2009 sind 64-Bit-Versionen von DataCore SANmelody und SANsymphony angekündigt, mit denen diese Grenze nicht mehr vorgegeben sein wird.

Nachdem nun aus physikalischem Speicherplatz ein virtuelles Volume erzeugt wurde, kann dieses einem Server zugewiesen werden. Typischerweise erfolgt diese Zuweisung über redundante Pfade, wobei es einen primären und mehrere sekundäre Pfade geben kann. Der Applikationsserver kommuniziert im Normalfall über den primären Pfad mit einem Speicherserver. Bei Schreibzugriffen werden die Daten zunächst im Cache des SDS abgelegt. Von hier erfolgt über einen zusätzlichen Mirrorpfad zwischen den SDS die Spiegelung der Daten in den Cache des zweiten SDS. Sobald dies erfolgreich war und dem ersten SDS bestätigt wurde, bekommt auch der Applikationsserver eine entsprechende Quittung zurückgeliefert und kann weitere Daten schreiben.

Sowohl SANmelody als auch SANsymphony nutzen Teile des Hauptspeichers für das Caching. IPStor von FalconStor verzichtet bewusst auf diese Funktionalität.

Am MPIDF werden sämtliche virtuellen Volumes synchron in einen zweiten Serverraum gespiegelt. Daher kommt für die SATA-Platten kein RAID-6 zum Einsatz, das sonst auf Grund der erfahrungsgemäß höheren Ausfallraten für diese Plattentechnologie in Betracht gezogen worden wäre.

6. Verfügbarkeit

Die am MPIDF realisierte Lösung bietet eine hohe Verfügbarkeit sowohl für die Server als auch die Speichersysteme.

Es existieren zwei Serverräume in unterschiedlichen Brandabschnitten. Serverraum 1 ist mit zwei VMware ESX-Servern, einem SDS, zwei Plattensystemen (SAS, SATA) sowie der entsprechenden Fibre-Channel-Infrastruktur ausgestattet. Serverraum 2 ist fast identisch bestückt. Sämtliche ESX-Server haben redundante Pfade zu beiden SANmelody-Servern. Als primärer Datenpfad ist jeweils derjenige SDS eingetragen, der sich im selben Serverraum befindet.

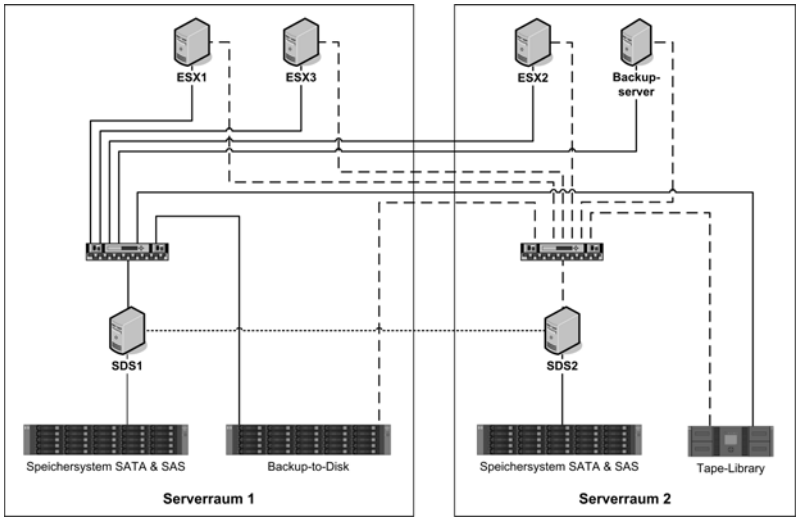


Abbildung 1: „SAN-Topologie“

Sollte es zu einem Ausfall eines VMware-Servers kommen, so wird dies über das VMware-Modul HA erkannt und die ausgefallenen virtuellen Server auf den verbleibenden ESX-Servern werden neu gestartet. Da sowohl die Betriebssysteme als auch die Anwendungen im SAN liegen, ist dies problemlos möglich. Die VMware-Server sind hinsichtlich Prozessor und

Arbeitsspeicher so konfiguriert, dass sogar nur ein Gerät alle virtuellen Server übergangsweise beherbergen kann.

Im laufenden Betrieb übernimmt das VMware-Modul DRS die Steuerung der Serverauslastung. Virtuelle Server können damit, z. B. für Wartungszwecke, im laufenden Betrieb auf einen anderen VMware-Server umgezogen werden.

Der Ausfall eines Speichergerätes oder eines SDS wird ebenfalls toleriert. Die Kommunikation zwischen VMware-Server und SDS erfolgt nun über den sekundären Pfad. Erkennt ein SDS den Ausfall seines Spiegelpartners, so wird das Caching beim Schreiben von Daten abgeschaltet. Die Schaffung von weiterer Redundanz ist durch das Hinzufügen von zusätzlichen Speicherservern möglich. Dies wurde am MPIDF jedoch nicht realisiert.

Zu Wartungszwecken ist auch im laufenden Betrieb die Abschaltung eines SDS möglich. SANmelody wird dazu gestoppt. Nach erfolgter Wartung und Neustart der Software wird automatisch eine Synchronisierung der Daten durchgeführt. In Abhängigkeit von der zwischenzeitlich angefallenen Datenmenge ist die Synchronisierung entweder vollständig oder inkrementell.

Die Datensicherung erfolgt ebenfalls redundant. Zunächst werden die Volumes aller virtuellen Server auf Festplatten gesichert, die sich im Serverraum 1 befinden. Die zur anschließenden Duplikation genutzten Bandlaufwerke sind in Serverraum 2 installiert. Tresore für die Archivbänder sind ebenfalls in unterschiedlichen Brandabschnitten vorhanden.

7. AutoProvisioning

Im Rahmen der Storagevirtualisierung eröffnet sich die Möglichkeit, den Applikationsservern mehr Speicher zur Verfügung zu stellen, als tatsächlich physikalisch vorhanden ist. Diese Funktionalität wird von den Herstellern unterschiedlich bezeichnet. DataCore benutzt den Begriff AutoProvisioning; bei FalconStor wird ThinProvisioning verwendet.

So kann z. B. eine 300 GB SAS-Platte als virtuelles Volume von 2 TB verwendet werden. Die Vorteile liegen in der vereinfachten Erweiterbarkeit des Gesamtsystems. Festplattenkapazität kann zu bestehenden Speicherpools hinzugefügt werden, ohne dass Veränderungen an den Applikationsservern notwendig sind.

Problematisch ist jedoch das Überschreiten der physischen Speichergrenze. Da das Betriebssystem des Applikationsservers diese Grenze nicht kennt, werden keine Schutzmechanismen aktiviert. Lediglich die ausbleibende Schreibquittung des SDS verhindert den Verlust von Daten.

Ähnliche Probleme entstehen auch, wenn mit hoher Frequenz Daten erzeugt und wieder gelöscht werden. Die Ursache dafür ist die langsame Freigabe von Speicher durch SANmelody. Nach dem Löschen von Daten steht der Speicherplatz nicht sofort wieder in vollem Umfang zur Verfügung, sondern wird nach und nach blockweise wieder gelöscht. Sollten nun neue Daten auf einen bereits sehr hoch ausgelasteten Speicherpool geschrieben werden, so besteht auch hier die Gefahr des Überschreitens der tatsächlich vorhandenen Festplattenkapazität.

AutoProvisioning scheint daher nur bei Servern mit langsam wachsender Datenmenge und guter Vorhersagemöglichkeit des Datenwachstums sinnvoll. Ein Beispiel am MPIDF ist Microsoft Exchange. Nach dem Löschen von Mails oder anderen Objekten werden freie Blöcke innerhalb der Datenbank generiert und von neuen Objekten belegt. Die Datenbank selbst wächst mit überschaubarer Geschwindigkeit.

8. Fazit

Die beschriebene Lösung ist am MPIDF seit ca. einem Jahr im produktiven Einsatz und funktioniert reibungslos. Die Installation wurde von Mitarbeitern der IT-Gruppe des MPIDF unter Anleitung eines von DataCore zertifizierten Technikers durchgeführt.

Alle beabsichtigten Ziele wie bessere Auslastung der Hardware, höhere Verfügbarkeit, Auslagerung von redundanten Systemen in einen zweiten Brandabschnitt und Ausbau der Speicherkapazität wurden erfüllt. Es gab bisher weder Datenverluste noch Nutzerbeschwerden.

Als problematisch, aber nicht unlösbar, stellte sich die 2-TB-Volumegrenze dar. So konnte die von DataCore empfohlene Umwandlung von physikalischen zu virtuellen Volumes im laufenden Betrieb am MPIDF nicht genutzt werden, da am Fileserver mehrere 2-TB-Volumes zu einem Volume-Set zusammengefasst sind. Stattdessen mussten die Daten auf den neuen Speicher kopiert werden. Ein weiterer Nachteil zeigte sich bei den Snapshots. Diese stehen unter SANmelody für Volume-Sets nicht zur Verfügung. Hier wäre ein Wechsel auf SANsymphony notwendig. Der Support durch DataCore zeigte sich bei allen Problemen zügig und kompetent.

Bisher konnten etwa 20 Server virtualisiert werden. Nur Server mit spezieller Hardware wie z. B. ISDN-Karten sind davon ausgenommen. Geräte mit seriellen Schnittstellen werden mit Hilfe von seriell-auf-Ethernet-Adaptern von LANtronix betrieben und stehen dadurch unabhängig vom VMware-Server allen virtuellen Servern zur Verfügung.

Prinzipiell besteht sogar die Möglichkeit, auch die SDS unter VMware zu betreiben. Da jedoch die Speichersysteme am MPIDF über SAS an die SDS angebunden sind, ist dies nicht möglich. Voraussetzung wären Speichergeräte mit Fibre-Channel-Schnittstelle.

Als nächster Schritt soll geprüft werden, inwiefern eine weitere Virtualisierung von Netzwerkinfrastruktur durchgeführt werden kann. Entsprechende Produkte liefern z. B. die Firmen Astaro oder Clavister mit ihren Firewalls. Gute Erfahrungen mit der Einbindung von VLANs auf den VMware-Servern liegen bereits vor.

Server Consolidation with Xen Farming

Ulrich Schwardmann

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Abstract

Most consolidation concepts for servers are based on virtualization of the underlying hardware components. This usually is implemented by either operating system-level virtualization, paravirtualization or virtual machines. All of these techniques are made flexible by allowing to implement a more or less broad variety of operating systems. This flexibility usually means individual administration of all these systems on the other hand.

But real server consolidation should be more comfortable for the administrator than just virtualizing the hardware: there should be an essential benefit in administration too. To our knowledge the only technique, except our proposal, that allowes an update mechanism, which is centralized on file system level, is the proprietary system Virtuozzo [1], that virtualizes on the operating system level. But in the open source path of this software, OpenVZ [2], this property is unfortunately not available.

The aim of this paper is to show a way to implement such a possibility of centralizing the update and installation mechanism to a group of xen instances on a xen server [3]. The main idea behind this concept is borrowed

from the technology of diskless clients. Like these diskless systems the xen clients all share a common file system that accommodates the main structure for the software components. Just the individual parts of the operating system and software components are hold in a special writable file system. Here in contrast to diskless clients a real file system is used, that additionally can hold the special software and data that is used on the individual client. In this file system of course all types of configuration and logging data is included.

This obviously means furthermore, that software installation and update cannot be done by the client on the central file system, but has to be done centrally on the so called master of this farm. A mayor part of the development of this farming was therefore a decision about the possibilities the client administrators should have and what the constraints due to the central management should be. Our viewpoint was, that the client administrators should concentrate on the application aspects. They should focus on the configuration of their needed software components and use the underlying operating system as a secure and updated basis.

This farming concept started at GWDG as a feasibility study, but is now in a state of hosting nine clients, with seven of them already in production. This paper describes the exact structure of the filesytem, the problem of data consistancy, the details of the boot process of the clients in order to get the whole file system available and the state of the utility components for installing and administrating master and clients.

1. The Concept

1.1 The Xen Servers Viewpoint

For the xen server itself there exist just a couple of xen clients, some of them working permanently, some started only for a very short time and shut down afterwards again.

These xen clients reside in a special network structure as shown in figure 1. The xen server bridges the clients external network connections and additionally the clients have an internal network interconnect, that is used to mount

the NFS share and for administration tasks, that can be executed from the xen server.

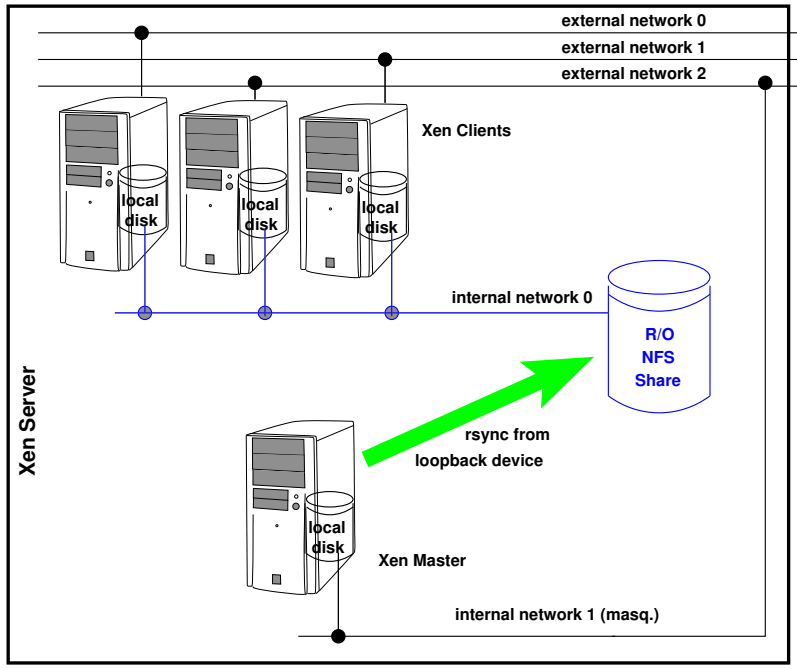


Figure 1: Logical structure of the clients and master and its network view

1.2 The Orchestration of the Xen Farm

The xen farm is orchestrated by a couple of simple shell scripts. These scripts are used to create the master, the clients, or the NFS share, to update or change these entities according to the changes made on the master, to control them or get access to them from the xen server. Furthermore there exists a configuration skript, that holds all variables used by these administration scripts.

1.3 The Clients Viewpoint

The client in a xen farm is a xen machine, that does not have write access to mayor parts of its installation. It imports these parts readonly from an NFS-server, as explained in section 2.1.

Already during the boot process at the init process of the initial RAM disk, the local part of the file system on virtual disk is enhanced by mounting the missing files of the read only part. This is done via NFS-mount to a special directory called `'/mroot'` for the masters root directory. This file system has to be accessible during the whole life time of the system, since all binaries, libraries etc., used in the system, are located there.

All services are configurable by their locally available configuration files. Data bases and software, that is not supported by the distribution used, can be installed into the local writeable disk space in `'/root'` or `'/usr/local'`.

1.4 The Necessity of a Network File System

Updates on the clients are mainly done on the readonly file system from outside, as decribed later in chapter 3.8.1. So the files in this file system change during the update process of a xen farm.

These changes during the runtime of the clients are the reason for the necessity of a NFS-mounted network file system, since these changes from outside have to be transparent to the operating system inside the clients. The file system has to have control of files, changed by processes outside the operating system, and the inodes, that point to these files and are currently used by processes inside the operating system.

Like the whole xen server itsself this NFS service can be a single point of failure, in case there is only one xen server used.

2. The File System Model

In order to find out, which parts of the server administration can be centralized and which parts have to be local, the main guideline is to distinguish between the centrally provided software itself and its configuration.

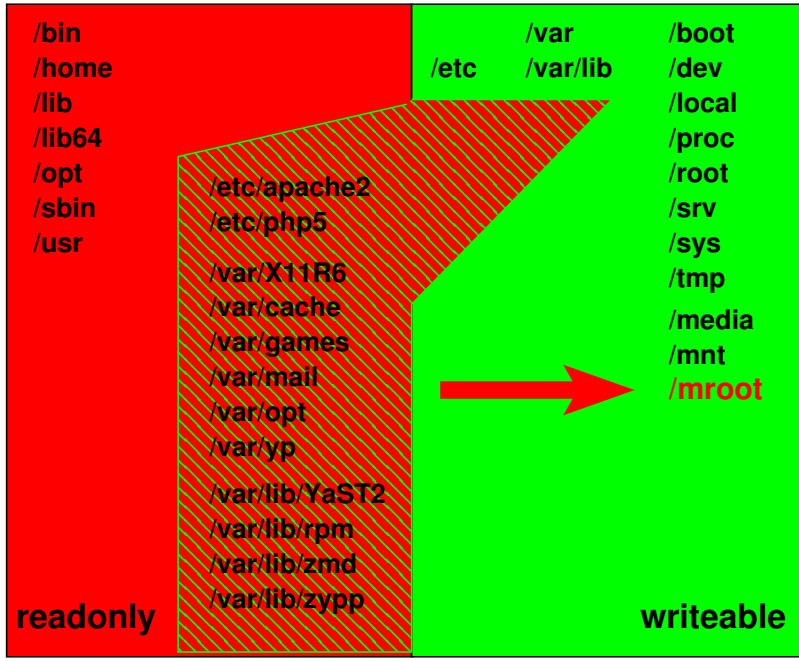


Figure 2: The structure of writable and read-only directories in the file system

2.1 Separation into Writable and Readonly Parts of the File System

Especially all containers of the software executables, libraries, static data etc. can be hold without write access of the clients administrator. All files that are changed by the operating system during its work, need obviously to have write access. Write access is needed furthermore for all areas with configuration files, that are meant to be changed for the user's needs. Since this is not everywhere consistently mapped into the directory structure of linux, one has to make some decisions here and there will be areas, that will not completely fit into this picture. The decision, which parts of the file system can be readonly and which parts have to be writable, depends to some extend on the choice of the linux distribution. Till now in this context there was only

the szenario with SuSE Linux Enterprise Server 10 [4] from Novell used. Especially in the `'/var'` subdirectories some changes might be necessary for other distributions.

The structure of read only and writeable directories and subdirectories chosen for the clients of the xen farm is shown in figure 2.

For the home directories the decision, whether they should be readonly or writeable, depends on its usage. In our local context we decided to use a preconfigured structure of mount points as read only directory. But there exist good reasons to use it as writeable area too.

2.2 Providing Space for Application Data

For the clients it should be possible to store application data. This type of data can be stored in a special writeable directory `'/local'`, which is the only directory that has a link backwards from the imported read only file system from `'/usr/local'` into the local writeable area. Beside the usual directories in `'/usr/local'` some additional are found here as `'etc'`, `'home'`, `'scratch'` or `'var'`. This list can be extended by the needs of the clients administrator.

3. The Technology

The first mayor problem here is, how the kernel gets access to both, the local disk and the remote NFS share during its boot process, i.e. before the init scripts need to use the files in the NFS share. Here an old concept of diskless clients provides the necessary technology.

3.1 The Concept of Diskless Clients

This concept (or the diskless X concept, called DXS) was developed in order to administrate a greater amount of computer, mainly used as X server, by one central NFS server, see [5] and [6].

The concept was used for the students computer pool at the University of Göttingen since 1998. The main advantage of this approach compared to a thin client or X terminal is, that the processes can have the full advantage of the local hardware and its peripherie and did not have to share it with others.

While these DXS got there complete network configuration, kernel, initial ram disk and file system via TFTP boot from the server, our concept only uses the technology developed for DXS to mount a remote file system into the initial ram disk and afterwards to remount it to the mountpoint used by the operating system

3.2 The Boot Process for the Xen Clients

The xen client has a special boot option for its individual internal network configuration, written in the ethernet option of its xen configuration file, that will be read by the init process of the initial ram disk. This option contains the ip-address, the NFS server, the gateway and the broadcast setting of this client, and can be found by the operating system in `´/proc/cmdline'`. The init process of the initial ram disk then can set up a network interface and the routing according to the settings of this kernel boot option.

Afterwards init starts the portmapper, loads the appropriate drivers for the NFS mount and mounts the readonly file system from the NFS server.

As a debugging function we included the possibility to interrupt the boot process at this point by starting a shell inside the init process of the initial ram disk. This option is implemented during the build process of the inititial ram disk.

When the initial ram disk continues at this point, it looks for an init binary on the root file system, typically found at '/sbin/init'. This file is already located in the readonly file system. Before the init script of the initial ram disk handles over to this init binary, the mount point of the readonly file system has to be moved to the correct place of the real operating system that starts afterwards.

From this point on everything continues as with a usual operating system init, despite the fact, that the data of most of the root file system is readonly and shared with others.

3.3 Setup of the Xen Server

The xen server is started just as in the generic xen server setup. The config files, images etc. are located as usual. It has a couple of xen clients to maintain, just as in an ordinary setup. There are only some requirements on the network, local bridge and firewall setup, that are described later.

3.4 Generate the Xen Master

Even the generation of a xen master is done in the standard manner by creation of a virtual disk and boot of an installation disk, that installs the favorite operating system. The only restriction here is, that the xen name of the xen master has to begin with `'master\_'` and a special environment variable `'DISTID'` has to be set in the configuration file `'xen\_cons.conf'`.

The content of the xen masters file system is basis of the NFS share that is exported as a readonly file system to the clients. The only difference to an ordinary file system of some distribution is, that there is a link from `'/usr/local'` to `'/local'` as it was mentioned before.

After the initialization the xen master it is powered down. It is only started, when its software stack has to be changed or updated.

An administration script for the masters setup together with the setup of the NFS share could be easily provided too, but is not part of the software at the moment.

3.5 Generate a Xen Client

This step is not as simple as the generation of the master, but it is already scripted. First a xen system that uses a readonly file system for most of its files is generated out of the content of the xen masters disk. There exists a script that performs this task. It starts with the generation of the xen clients configuration file, usually found in `'/etc/xen/vm'`. For this the external IP-address and the full qualified domain name are asked by the script. This name is used as internal xen name too, so the name of the config file has the same name. Additionally the wanted disk size and the name of the application administrators email address are asked here. This is a useful information for central administration purposes.

In the next step the script generates free IP address for the internal network interface and MAC addresses for the external and internal interfaces, and a unique xen id: `'XEN\_UUID'`.

These parameters are tested on consistency before the xen configuration file is written and the network configuration is stored to some special files for later use. Now the initial ram disk of the xen masters kernel is adapted. Afterwards the disk is generated with root file system and swap space, and populated with those files, that are determined to be local and writeable. At this point the only files, that are special to this xen client, are the configuration files for the network settings. From the software point of view the client is a clone of the master.

3.6 Setup of the NFS Share

The NFS share resides in the center of the xen farming concept. But conceptually it is fairly simple. It contains the complete root file system of the xen master. The structure to find the missing parts of the clients file system is completely incorporated in the writeable part of the clients file system. For

the first setup of this file system the masters root file system is completely copied. Later it sufficies to synchronize these two file systems, whenever there was an update of the xen master.

This synchronization must be done by the xen and NFS server since this is the only instance, that has write access to the NFS share. The xen server therefore mounts the xen masters virtual file system as loopback device from the virtual disk and synchronizes this to the NFS share. At the moment the file systems name can be chosen as a variable of the configuration script. If the xen server should populate more than one xen farm, one has to use two different file systems as NFS shares and at the moment one has to use two different sets of administration and configurations scripts too.

3.7 Disk Usage of Writable and Readonly Parts of the File System

In the current installation of the xen farm, based on a rather complete software stack of a SuSE Linux Enterprise Server 10 [4] operating system, we have a disk usage of about 4.5 GB in the read only area and about 150 MB in the read only area after initiating a new client.

It is recommended to configure the clients local and writeable diskspace with 1 GB or more, since file systems like `'/proc'`, that are populated by the operating system during runtime need already about 300 MB.

3.8 Update of the Xen Farm

The update of the operating system as well as all other changes in the software stack of the xen farm is performed in four steps:

3.8.1 Update of the Xen Master

Because the xen master is usually offline, the first that has to be done is to start it. Afterwards in this virtual machine all necessary or wanted updates are performed as in a usual xen client.

There is a slight difference for the case of a kernel update, that additionally comes with an update of the kernel modules found in `'/lib/modules'`, and usually this way the old modules will be deleted. In order to grant the running kernel on the client systems further access to its modules, this modules directory is moved away and back again during the update process of the master.

3.8.2 Update of the NFS Share

After this the xen machine of the master is shutted down and the xen server synchronizes the NFS share from the loopback mounted virtual disk of the xen master. This automatically updates all files in the readonly part of the clients file system. by the properties of the network file system.

3.8.3 Update of the initial ram disk and the kernel modules

Whenever a new kernel is installed during the update of the master, a new initial ram disk comes with it. In this environment we need a modified one, therefore this modification has to be done inside the new initial ram disk after the update process.

Since the kernel modules of old kernels were saved in the masters file system, the old modules stay in the NFS share too. So it is not necessary to restart the clients immediatly after an update of the master and the xen farm, but it should be done as soon as possible, since a kernel update is most often a security udate. But this way the reboot can be planned by the clients administrators due to their needs. They just have to get informed.

3.8.4 Update of the Xen Clients

After all this there are still open the changes that where done in the masters file system, that belong to those parts, that are local and writeable to the clients.

In order to find out, what changes are done by the administrator already and what files are updated by the update process on the master, a complete check on differences between all files of the writeable part of the client with the corresponding files in the masters copy is done in advance on all clients before the update of the master is started. After the update all files, that did not differ before and differ now are replaced, because they have been untouched by the administrator. Those local files that differ from the masters copy are assumed to be changed by the administrator. Here the adminstrator has the possibility, to decide whether those files should be replaced by the update process or not. This decision has to be specified in the file `'/etc/nosync'`, that counts all files that should be left untouched. But because it is often necessary for the administrator to be informed about files, which changes are done by the update process, a copy of the updated version of those files with an appendix to the name (`.xennew`). All the other differing files are replaced by the new version, but the old version is saved before to a file again with an appendix to the name (`.xensave`).

3.9 Administration of the Xen Farm

Even if the advantage of a central administration of such a xen farm is conceptually clear, it is necessary, to have a couple of tools, that are able to maintain this farm. At the moment there are scripts for the following tasks:

- build a xen client
- delete a xen client
- exec a command on all or one client
- update xen master, NFS share and all clients
- build a new initial ram disk (as part of the update process)
- build a backup of all clients (see below)
- show network configuration or the administrators email address
- notification of the admins about important issues (kernel updates, xen server reboot etc.)
- an integration into the virtual machine manager API [7]

What is still missing at the moment:

- build a xen master, together with an NFS share
- central control of kernel modifications
- migrating the clients of the xen farm
- availibility concepts

4. Conclusion and Further Outlook

First this xen farming concept was implemented at GWDG as a feasiblity study, but it is now already since nearly one year with seven xen clients in production. It is installed on two xen server. These two server are used in a redundancy mode and to migrate clients for load balancing. The operating system of master and clients is only tested for SuSE Linux Enterprise Server 10 [4], but it should work for other distributions with minor adaptions. The software of this project is open and can be obtained directly from the author.

Bibliography

[1] Virtuozzo, Virtualisation Concept: http://www.parallels.com/de/products/virtuozzo/os/

[2] OpenVZ: http://wiki.openvz.org/

[3] Xen: http://xen.org/

[4] Novell, SuSE Linux Enterprise Server 10: http://www.novell.com/products/server/

[5] Dirk von Suchodoletz: Effizienter Betrieb großer Rechnerpools, Implementierung am Beispiel des Studierendennetzes an der Universität Göttingen, GWDG-Bericht Nr. 59, 2003, ISSN 0176-2516, pp. 271+X.

[6] Dirk von Suchodoletz: Thin-Clients - Plattenloser Arbeitsplatz selbstgemacht, Linux-Magazin 2000/08, pp.110-115.

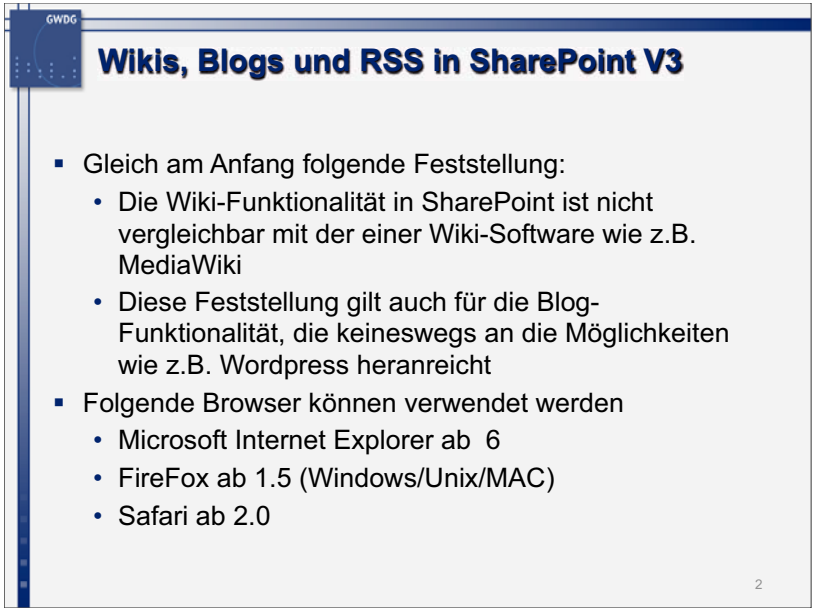
[7] Virtual Machine Manager: http://virt-manager.org

Wikis, Blogs und RSS in SharePoint V3

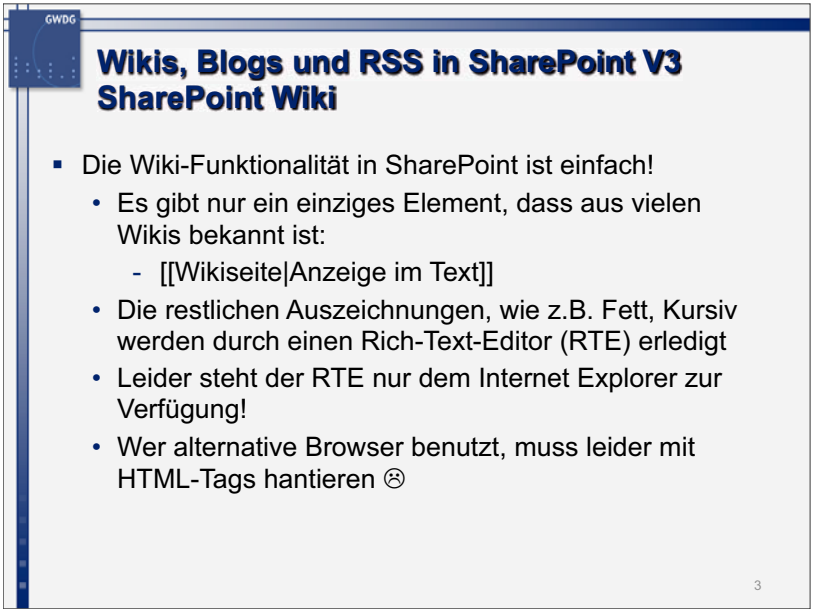
Thorsten Hindermann

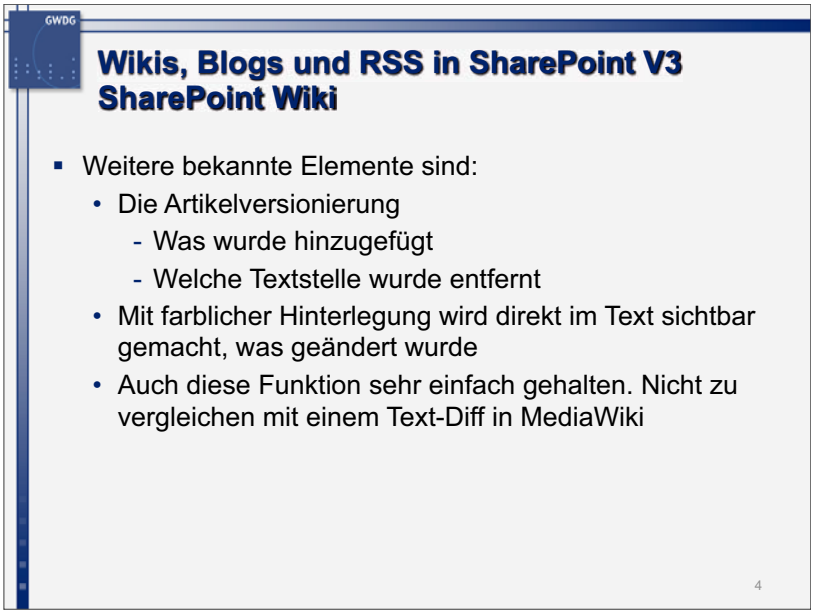
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Jede Firma möchte in der heutigen Zeit mit auf den Web-2.0-Zug aufspringen, um dabei zu sein. Im Web-2.0-Umfeld haben sich Wikis, Blogs und RSS-Feeds als Synonym für diese neue Art, mit und im Web zu arbeiten, herauskristallisiert. Auch die Firma Microsoft möchte da nicht hinten anstehen, sondern mittendrin dabei sein. Also hat Microsoft seine Kollaborationssoftware um eben diese drei Web-2.0-Möglichkeiten erweitert. Leider hat sie diese neuen Möglichkeiten nicht bis ganz zu Ende verarbeitet, sondern ist in der Mitte stehen geblieben, so dass nur kleine Lösungen dieser ansonsten fantastischen Möglichkeiten implementiert wurden. Einzig die Unterstützung der Browser ist schon ein Novum für Microsoft, neben dem Internet Explorer (IE) auch noch andere Browser zum Zugriff auf SharePoint zuzulassen.



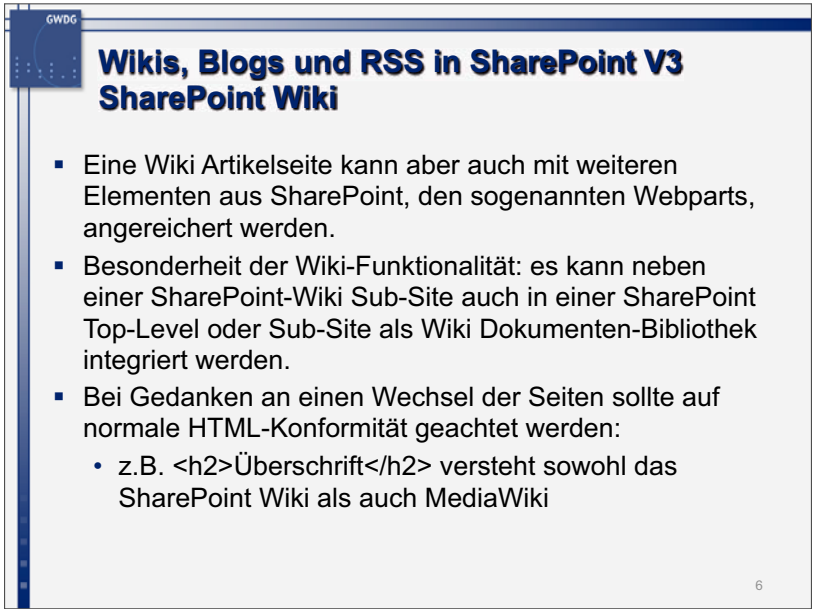
Im Folgenden werden die einfachen Möglichkeiten des SharePoint Wiki beschrieben:





Eine SharePoint-spezifische Eingliederung der Wiki-Funktionalität wird in der nächsten Folie beschrieben. Ein interessantes Feature bei SharePoint ist die Vergabe von Berechtigungen bis auf Seiten-Ebene herunter. In einem „normalen“ Wiki gibt es ja solche Einschränkungen kaum oder gar nicht. Vom Wiki-Gedanken aus gesehen ist das ja auch genau richtig, aber im Firmeneinsatz ist doch oftmals eine Berechtigungsstruktur gewünscht. Hier kann das SharePoint Wiki mit seiner integrierten Berechtigungsstruktur auftrumpfen.

Durch die Integration in SharePoint stehen aber auch noch spezifische Möglichkeiten zur Verfügung, über die andere Wikis so in dieser Art nicht verfügen.



Bei der Blog-Funktionalität in SharePoint ist es ähnlich wie beim Wiki – einfach gehalten und integrierte Rechteverwaltung. In der Folie wird darauf hingewiesen, das mit dem IE mehr inhaltlich gestaltet werden kann, als mit anderen Browsern – Stichwort RTE (Rich Text Editor):

Die weiteren Möglichkeiten des SharePoint Blogs werden in der folgenden Folie aufgezeigt:

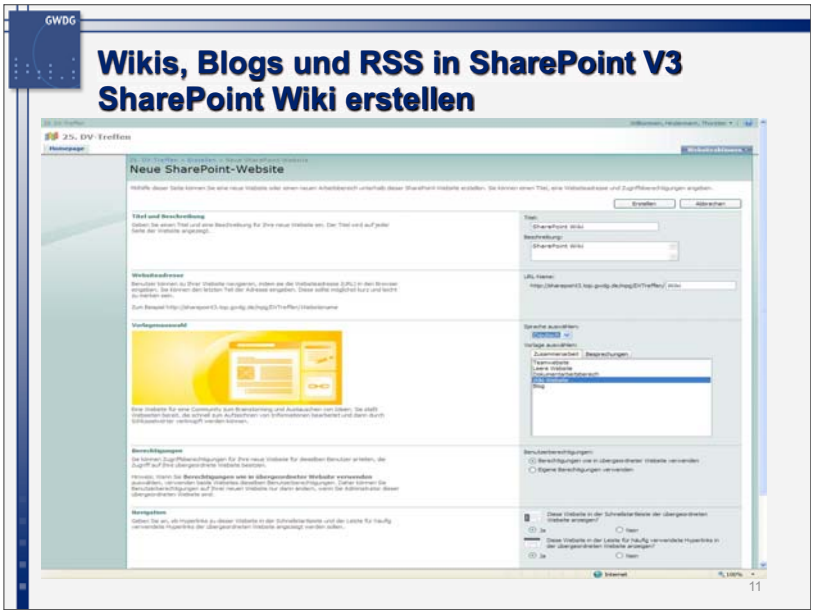
Im letzen Punkt wird noch darauf hingewiesen, dass neben der Blogbeitragseinstellung mit einem Webbrowser auch die Programme Word 2007 und Windows Live Writer die Möglichkeit bieten, in den SharePoint Blog Beiträge einzustellen.

Die Möglichkeit der RSS-Feedunterstützung von SharePoint in der Version 3 wird in dieser Folie dargestellt:

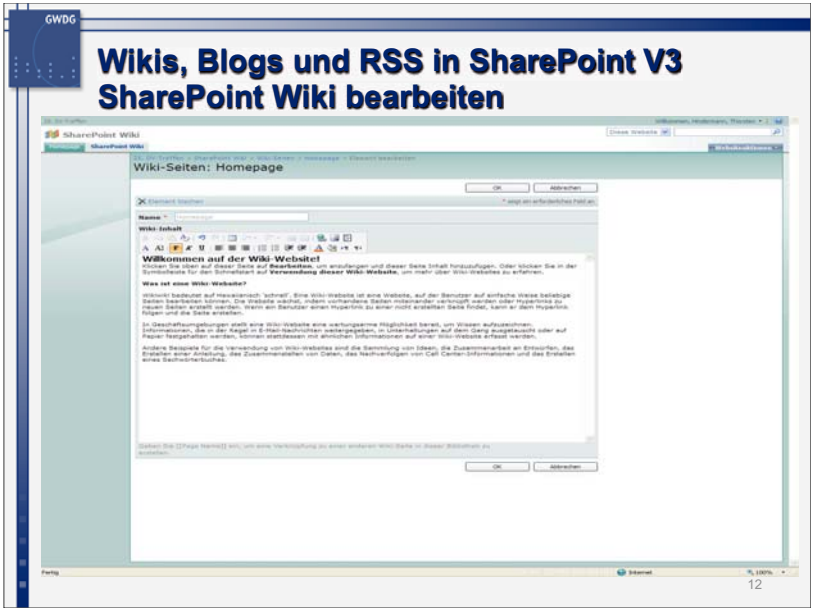
Auf der vorigen Folie werden im Fazit noch einmal ein paar Kernpunkte zusammengefasst aufgelistet.

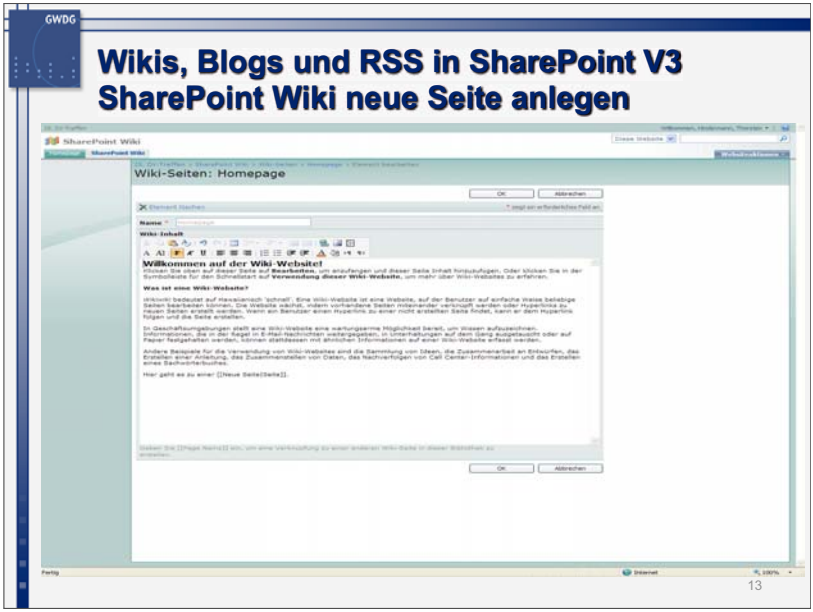
Im folgenden „Praxis“-Teil zeigen die Folien die Erstellung und die Arbeit mit der Wiki-, Blog- und RSS-Funktionalität.

Ein SharePoint-Wiki-Bereich wird erstellt:

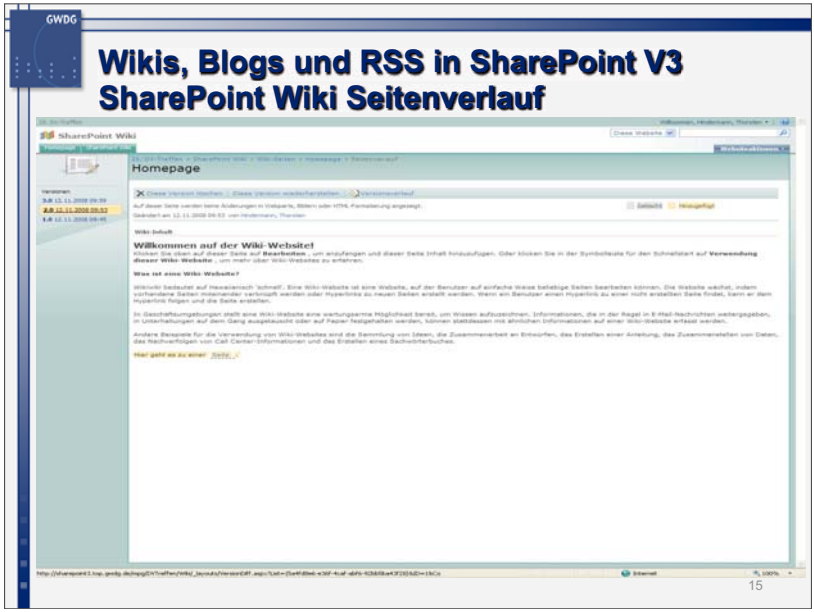


Die Bearbeitung und das Anlegen einer neuen Seite werden in den folgenden drei Folien gezeigt:

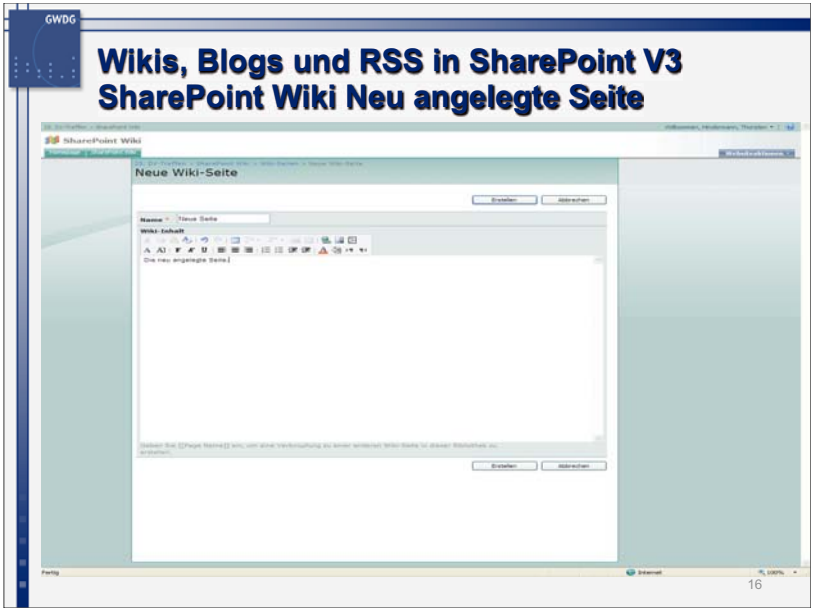


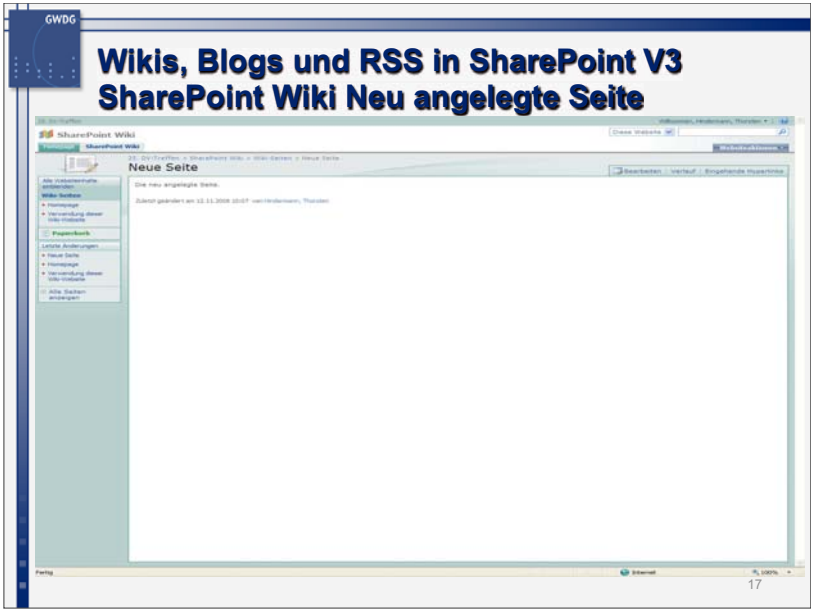


Die Funktionalität der Seitenhistorie wird gezeigt:



Die Bearbeitung der neu angelegten Seite wird betrachtet:

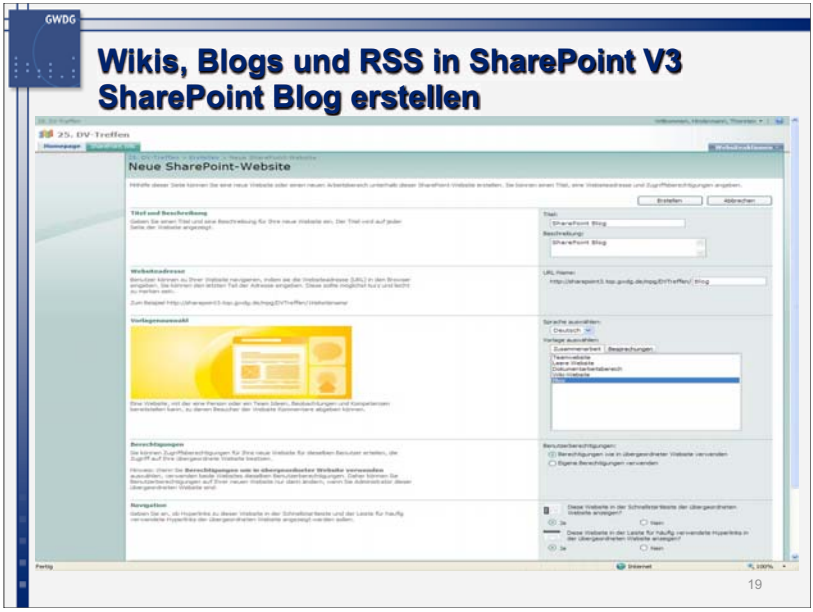




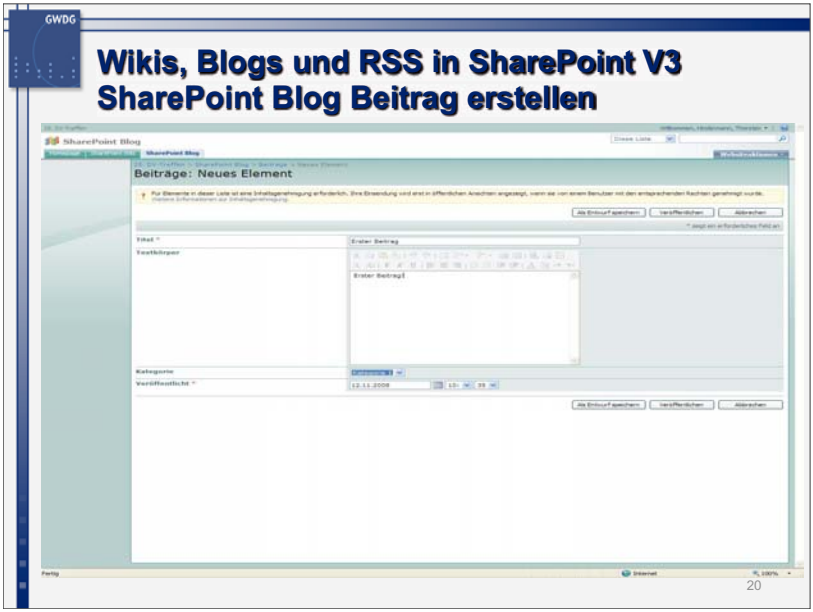
Und schließlich wird die Portierung eines SharePoint-Wiki-Seiteninhaltes in eine MediaWiki-Seite gezeigt.

Hiermit bietet sich die Möglichkeit, später SharePoint-Wiki-Seiteninhalte in eine andere Wiki-Software zu portieren, in diesem Beispiel in die Media-Wiki-Software.

Die Erstellung eines SharePoint Blogs wird dargestellt:

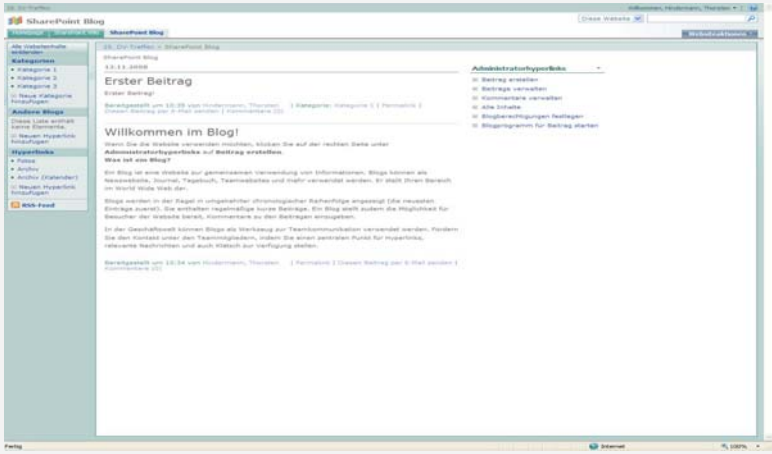


In den nächsten Folien wird gezeigt, wie ein neuer Blogeintrag und -kommentar mit einem Webbrowser eingestellt werden:



GWDG

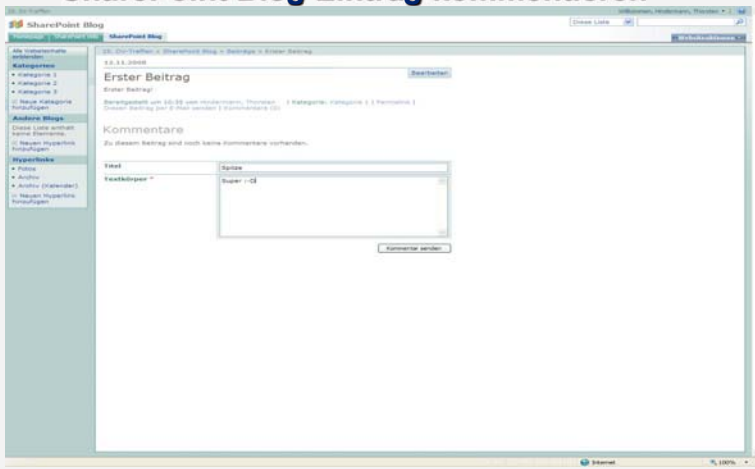
Wikis, Blogs und RSS in SharePoint V3
SharePoint Blog erster Beitrag veröffentlicht



21

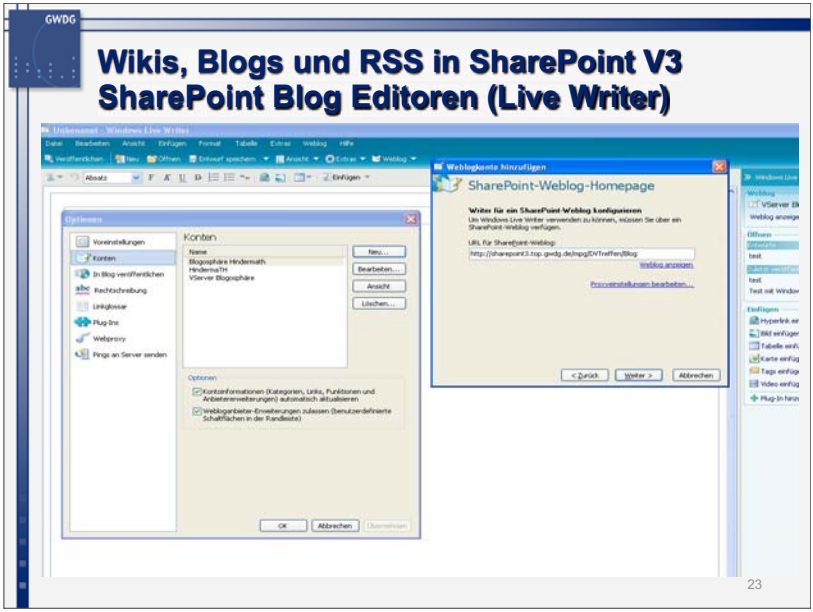
GWDG

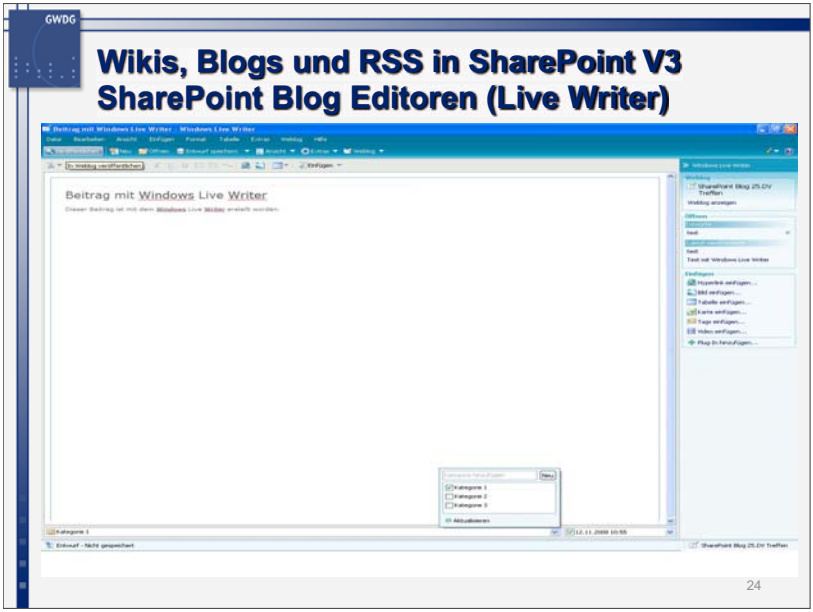
Wikis, Blogs und RSS in SharePoint V3
SharePoint Blog Eintrag kommentieren

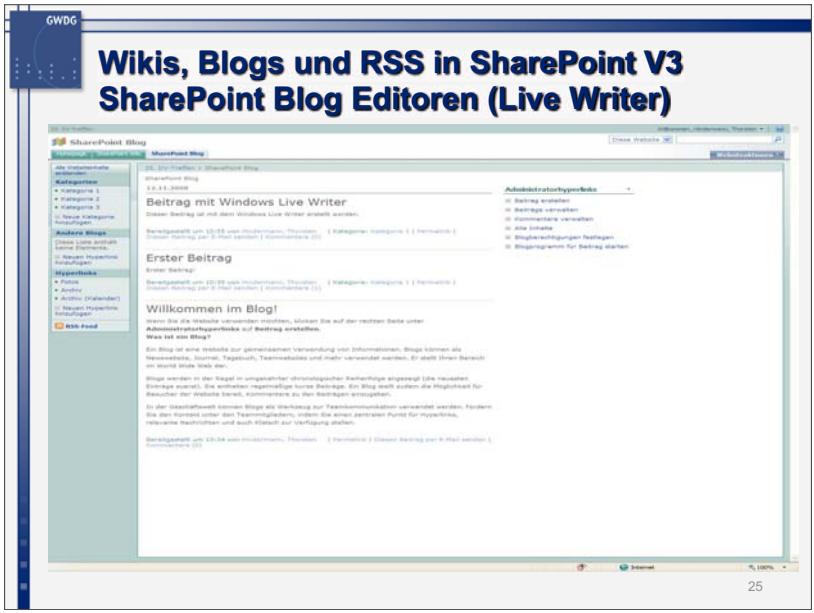


22

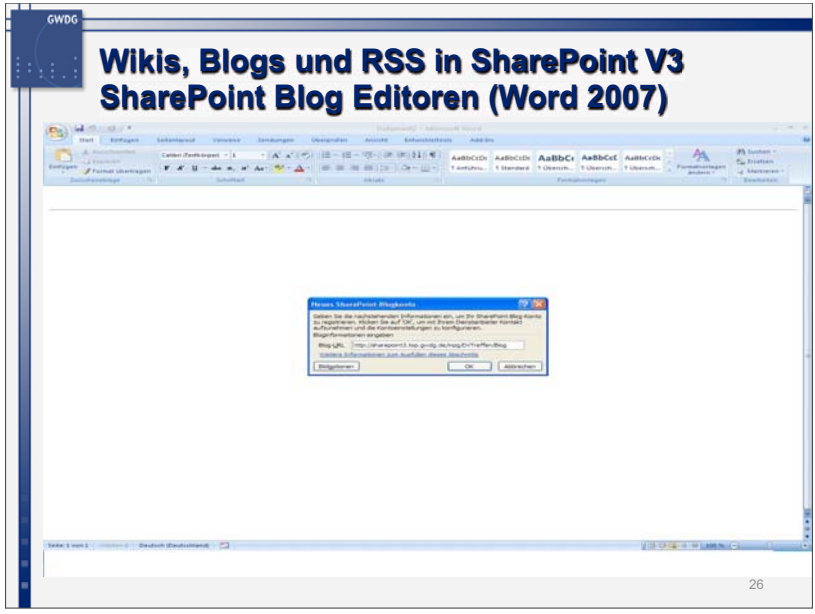
Wie Blogeinträge mit dem Windows Live Writer in einen SharePoint Blog eingestellt werden, zeigen die nächsten Folien:





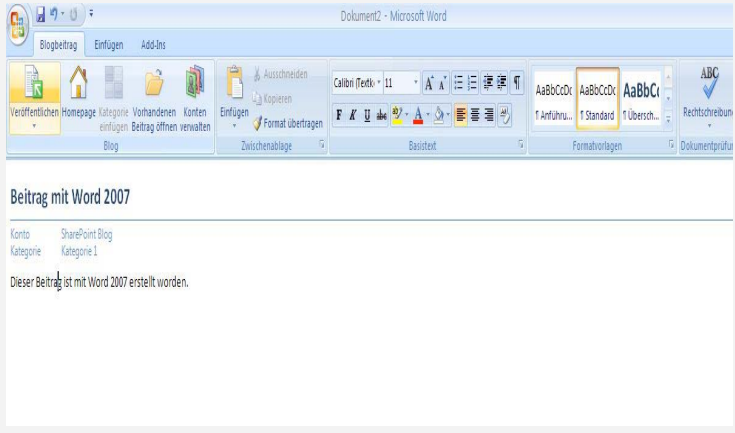


Weiterhin wird diese Möglichkeit auch mit Word 2007 demonstriert:



GWDG

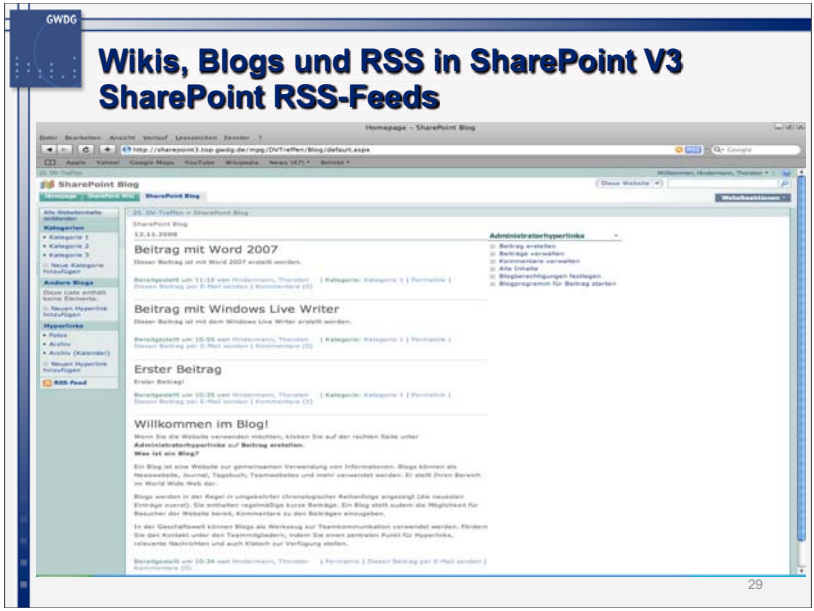
Wikis, Blogs und RSS in SharePoint V3
SharePoint Blog Editoren (Word 2007)

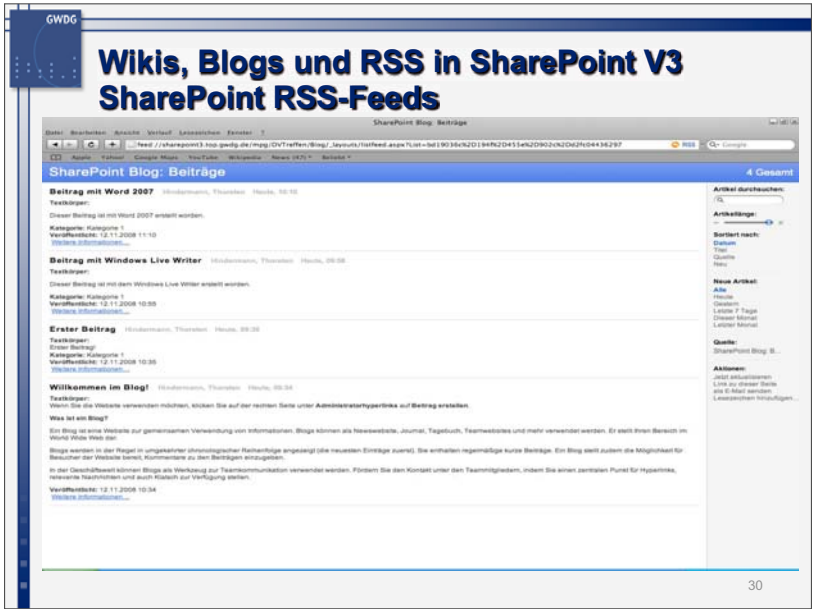


GWDG

Wikis, Blogs und RSS in SharePoint V3
SharePoint Blog Editoren (Word 2007)

In den letzen beiden Folien wird die RSS-Feed-Funktionalität mit dem Safari Webbrowser gezeigt:





Dezentrale Authentifizierung für Web-Anwendungen mit SAML und OpenID

Sebastian Rieger

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Einleitung

Unterstützt durch Entwicklungen wie z. B. dem „Web 2.0“ haben die Anzahl und Komplexität von Web-Anwendungen in den letzten Jahren stark zugenommen. Dabei übernehmen Web-Anwendungen zunehmend auch Aufgaben, die zuvor Desktop-Anwendungen vorbehalten waren. Viele dieser Web-Anwendungen verwalten zudem private bzw. vor dem Zugriff durch Dritte zu schützende Daten und erfordern daher vor der Verwendung eine erfolgreiche Authentifizierung und Autorisierung der Benutzer. Die Anwender müssen für jede Applikation Benutzernamen und Passwörter verwalten, was neben dem erhöhten Aufwand bei der Verwendung der Web-Applikation auch Auswirkungen auf die Sicherheit haben kann, sofern die Benutzer infolgedessen für alle Anwendungen die gleichen bzw. einfache Passwörter definieren. Die Vereinheitlichung der Verwaltung der Identitäten durch die Benutzer sowie auf der Seite der Betreiber der Anwendungen bildet das Umfeld für das Identity Management (IdM). Zentralistische IdM-Lösungen sind jedoch für dezentrale Web-Anwendungen nur bedingt verwendbar. Daher haben sich seit einigen Jahren mit der Security Assertion Markup

Language (SAML) [1] sowie dem OpenID-Standard [2] zwei dezentrale IdM-Ansätze für Web-Anwendungen etabliert. Gemeinsam mit dem Rechenzentrum Garching betreibt die GWDG eine auf SAML-basierende Lösung (MPG-AAI [3]) für Web-Anwendungen der Max-Planck-Gesellschaft. Dieser Beitrag schildert die Vor- und Nachteile der konkurrierenden Ansätze SAML und OpenID und zeigt Möglichkeiten für die Integration beider Verfahren in der MPG-AAI.

2. Evolution des Identity Managements

Um die Verwaltung von Identitäten (z. B. Benutzernamen und Passwörtern) auf der Seite der Benutzer sowie der Betreiber zu vereinheitlichen, existieren unterschiedliche Verfahren, die unter dem Begriff Identity Management (IdM) zusammengefasst werden können [4]. Das IdM zielt hierbei auf eine Verminderung des Aufwands bei der Authentifizierung, Autorisierung sowie dem Accounting von Benutzern. Häufig soll in Bezug auf die Authentifizierung ein einheitlicher Benutzername bzw. ein einheitliches Passwort („Single Username“, „Single Password“) erzielt oder durch eine einzige Anmeldung mehrere Anwendungen verwendet werden können („Single Sign-On“, kurz SSO). In der Vergangenheit wurden einheitliche Benutzernamen und Passwörter durch die Realisierung zentraler Dienste (z. B. NIS, Verzeichnisdienste etc.) etabliert. Auch für die Verwendung unterschiedlicher Web-Anwendungen wurden zentrale Verzeichnisse konzipiert (vgl. z. B. Microsoft Passport [5]). Diese Zentralisierung erleichtert den Betrieb zentraler IT-Infrastrukturen, weist allerdings zwei Probleme bei der Anbindung externer Benutzer (z. B. von Kooperationspartnern, Kunden usw.) auf. Einerseits werden nicht nur die Dienste, sondern auch die darin gespeicherten Daten zentralisiert (vgl. einem Datensilo), was aus Sicht des Datenschutzes bei zunehmenden Benutzerzahlen aus unterschiedlichen Einrichtungen inakzeptabel sein kann. Andererseits handelt es sich bezogen auf ein standortübergreifendes IdM um Insel-Lösungen, die häufig untereinander nicht kompatibel sind. Außerdem müssten bei einer Kooperation alle Benutzer der Kooperationspartner in allen zentralen Diensten an den einzelnen Standorten repliziert und verwaltet werden. Um die Skalierbarkeit der Dienste bezüglich externer Benutzer zu erhöhen, wurden IdM-Lösungen entwickelt (zunächst zentral z. B. als Meta-Directory, Virtual Directory, LDAP oder RADIUS Proxy) [6]. Auch diese setzen allerdings kompatible Verfahren für die Authentifizierung und Autorisierung voraus oder erfordern die standortübergreifende Synchronisation und Verwaltung von Identitäten. Um dezentralen Benutzergruppen Zugriff auf dezentrale Anwendungen zu ermöglichen, ist zunehmend eine Dezentralisierung des IdM erforderlich, wie sie in der Abbildung 1 dargestellt ist:

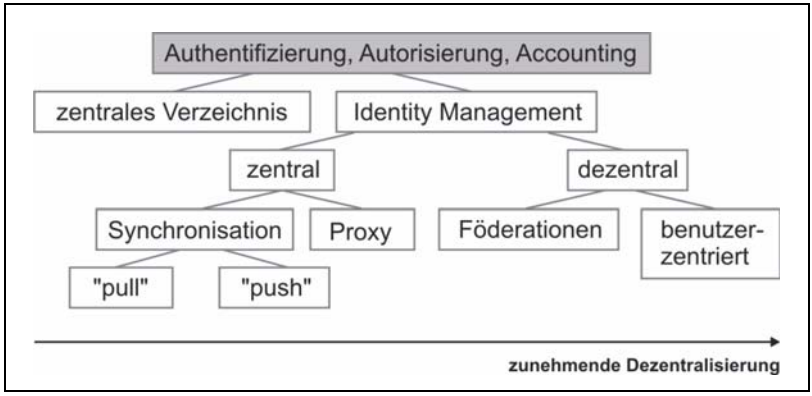


Abb. 1: Dezentralisierung des Identity Managements

Für die dezentrale Authentifizierung existieren bereits einheitliche Verfahren wie z. B. Kerberos [7] oder X.509-Zertifikate [8]. Durch Trust-Beziehungen lässt sich in einer Kerberos-Umgebung oder einer Public-Key-Infrastruktur die dezentrale Verwaltung von Benutzeridentitäten erzielen. Diese lassen sich jedoch nur bedingt für die Autorisierung verwenden und erfordern erneut einheitliche Verfahren und erleichtern die Zentralisierung der verwendeten Daten (z. B. des Benutzernamens). Geeignete Verfahren für ein vollständig dezentrales Identity Management für Web-Anwendungen lassen sich derzeit in zwei Kategorien einteilen. Zum einen können mehrere Partner (Anbieter von Anwendungen und Benutzer unterschiedlicher Organisationen) ihre Identitäten föderieren („federated identity“) [4]. Beispielsweise existiert für das deutsche Forschungsnetz die vom DFN-Verein betriebene DFN-AAI (Authentifizierungs- und Autorisierungs-Infrastruktur) [9]. Für die Anwendungen der Institute und Partner der Max-Planck-Gesellschaft betreibt die GWDG gemeinsam mit dem Rechenzentrum Garching die Föderation MPG-AAI. Durch die Föderation wird das IdM unterschiedlicher Standorte verbunden. Die Föderation bildet eine Vertrauensgrundlage, die juristisch auf einer zugehörigen Policy und technisch auf der Prüfung von digitalen Signaturen (X.509-Zertifikaten) beruht. Als Standard für Föderationen wurde von der Organization for the Advancement of Structured Information Standards (OASIS) die Security Assertion Markup Language (SAML) in der aktuellen Version 2.0 [1] spezifiziert. Auf SAML basierende Implementierungen bieten z. B. Shibboleth [10], simpleSAMLphp [11], ADFS [12] oder Liberty [13].

Als Alternative zur föderativen Authentifizierung wurden in den letzten Jahren Verfahren entwickelt, die die Dezentralisierung der Verwaltung der Iden-

titäten weiter ausbauen und sie auf den Benutzer verlagern. Man spricht in diesem Zusammenhang von benutzerzentriertem („user-centric“) IdM. Derzeit existieren unterschiedliche Standards und Implementierungen wie z. B. OpenID [2], CardSpace [14], OAuth [15], sxip [16] und higgins [17]. Seit 2008 hat insbesondere die Verbreitung von OpenID stark zugenommen. OpenID fokussiert genau wie SAML derzeit vorrangig Web-Anwendungen.

3. Föderative Authentifizierung mit SAML

Bei der föderativen Authentifizierung werden bei der Durchführung der Authentifizierung und Autorisierung zwei Parteien unterschieden. Der sog. Service Provider (SP) stellt eine Anwendung zur Verfügung und führt die Autorisierung berechtigter Benutzer durch. Er verwaltet jedoch keine Benutzeridentitäten bzw. Benutzernamen und Passwörter. Diese verbleiben in der „Heimat-Organisation“ des Benutzers bzw. seiner Institution, die ihrerseits einen Identity Provider (IdP) betreibt, der an der Föderation teilnimmt. Innerhalb der Föderation vertrauen sich mehrere SPs und IdPs. SPs vertrauen bei der Autorisierung der Benutzer auf die durch eine digitale Signatur überprüfbare erfolgreiche Authentifizierung der Benutzer am IdP ihrer Heimat-Organisation. Der IdP liefert dem SP darüber hinaus für die Autorisierung innerhalb der Föderation standardisierte Attribute des Benutzers. Diese basieren z. B. auf dem eduPerson-Standard [18] (z. B. als eduPersonEntitlement „common-lib-terms“). Die Einhaltung der Attribute sowie letztlich das Vertrauen der SPs und IdPs innerhalb der Föderation sind neben der technischen Implementierung anhand digitaler Zertifikate (z. B. aus der DFN-PKI [19]) über die Policy (Richtlinien) der Föderation definiert, die von den Betreibern von Diensten in der Föderation eingehalten werden müssen. Benutzer können nach einmaliger erfolgreicher Anmeldung am IdP ihrer Heimat-Organisation alle SPs der Föderation verwenden, ohne sich erneut anmelden zu müssen (Single Sign-On).

Der SAML-Standard der OASIS gewährleistet hierbei sowohl die Kompatibilität der verwendeten Authentifizierungs- und Autorisierungsverfahren (vgl. SAML-Profile [1]) als auch der ausgetauschten Informationen (sog. Assertions bzw. Tokens).

3.1 Shibboleth 2.0

Abbildung 2 zeigt den Ablauf einer SAML-basierten Authentifizierung und Autorisierung am Beispiel der Implementierung Shibboleth in der Version 2.0 [10]:

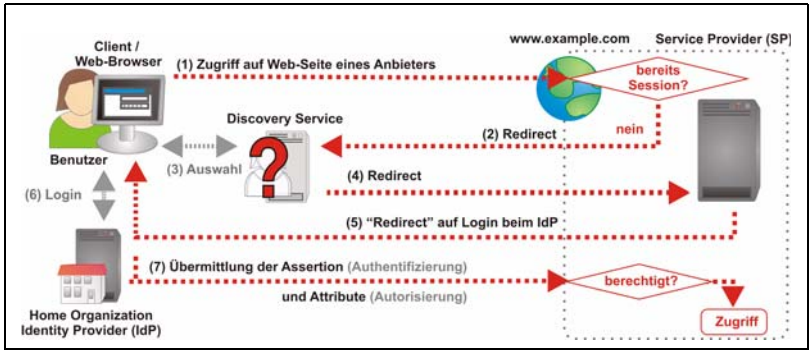


Abb. 2: Föderative Authentifizierung am Beispiel von Shibboleth 2.0

Zunächst greift der Benutzer hierbei auf eine Ressource bzw. Web-Anwendung zu, die auf einem SP liegt. Existiert für den Benutzer bereits eine gültige Sitzung (die anhand des übermittelten HTTP-Cookies [20] ermittelt werden kann), so erhält dieser direkt Zugriff auf die gewünschte Ressource. Greift der Benutzer jedoch zum ersten Mal auf die Ressource zu, erfolgt dessen Authentifizierung und Autorisierung. Hierfür leitet der SP den Benutzer an den Discovery Service (vormals „Where Are You From?“ bzw. WAYF-Server) der Föderation um. Der Benutzer wählt bei dem Discovery Service seine Heimat-Organisation aus, an der er sich authentifizieren möchte. Er kann die Auswahl speichern, so dass innerhalb der Föderation später keine erneute Selektion seiner Heimat-Organisation am Discovery Service mehr erforderlich ist. Der Discovery Service leitet den Web-Browser des Benutzers anschließend zurück zum SP um, der seinerseits, sofern er die Auswahl akzeptiert, eine Umleitung auf den zur gewählten Heimat-Organisation gehörigen IdP vornimmt.

Sofern der Benutzer am IdP noch keine gültige Sitzung hat, wird er aufgefordert, sich anzumelden. Die Authentifizierung kann hierbei gegenüber dem lokalen IdM bzw. einem Verzeichnisdienst erfolgen. Nach erfolgreicher Authentifizierung am IdP übermittelt dieser ein digital signiertes Token (Assertion) an den Benutzer, dessen Browser diese automatisch an den SP umleitet. Der SP prüft schließlich die Signatur des IdP und führt anhand der übermittelten Attribute die Autorisierung des Benutzers durch. Ist auch diese erfolgreich, erhält der Benutzer Zugriff auf die gewünschte Ressource.

Durch die Umleitungen des Web-Browsers des Benutzers zwischen den einzelnen Parteien und die dabei verwendeten Web-Sitzungen (basierend auf HTTP-Cookies) wird ein Single Sign-On ermöglicht, das dem Benutzer nach

einmaliger Auswahl seines IdP und dortiger Anmeldung alle Dienste (SPs) in der Föderation zur Verfügung stellt, ohne ein weiteres Login zu erfordern.

3.2 Probleme der föderativen Authentifizierung

Die in den vorherigen Abschnitten beschriebene Lösung für ein auf Föderationen basierendes dezentrales Identity Management weist in der Praxis einige Probleme auf. Ein Problem besteht in der Tatsache, dass mehrere Föderationen existieren können und Benutzer möglicherweise Dienste in unterschiedlichen Föderationen verwenden können müssen. Als Lösungsansatz können SPs und IdPs hierfür in mehrere Föderationen integriert werden. Außerdem existiert mit eduGAIN [21] ein Ansatz, der mehrere Föderationen untereinander zu einer Konföderation verbindet.

Ein weiteres Problem bildet die Usability der föderativen Authentifizierung. Benutzer müssen bei der Verwendung ihre Föderation und Heimat-Organisation kennen und auswählen. SAML ist zudem momentan nur für Web-Anwendungen implementiert. Allerdings existieren Konzepte für die Verwendung in Grid- [22] oder Desktop-Anwendungen [23]. Während ein Single Sign-On erreicht wird, ist das einheitliche Abmelden („Single Logout“) auch in Shibboleth 2.0 noch nicht vollständig implementiert. Der Benutzer muss seinen Web-Browser vollständig beenden, um alle Sitzungen zu beenden und seine Daten vor dem Zugriff durch Dritte zu schützen. Die persönlichen Daten des Benutzers verlassen zusätzlich in Form der Attribute des Benutzers die Heimat-Organisation und werden bei unterschiedlichen SPs gespeichert. SPs können damit ein Profil des Anwenders und dessen Nutzungsverhalten über unterschiedliche Anwendungen ermitteln. Um hier den Datenschutz zu erhöhen, bietet Shibboleth die Möglichkeit, Attribute nur an bestimmte SPs zu übermitteln (Attribute Release Policy, kurz: ARP), allerdings werden Benutzernamen etc. häufig an alle SPs übermittelt. Eine bessere Lösung bietet die Shibboleth-Erweiterung uApprove der SWITCHaai [24]. Hierbei muss der Benutzer der Übermittlung der Attribute an jeden SP einmalig explizit zustimmen und erhält somit nicht nur Auskunft, sondern auch Kontrolle über die übermittelten Daten. Häufig werden auch pseudonymisierte Attribute (z. B. eine persistente ID anstelle des Benutzernamens) verwendet. Diese erschweren jedoch wiederum das Accounting, da der Nutzer und die damit verbundene Kostenstelle nicht mehr ermittelt werden können.

4. Benutzerzentrierte Authentifizierung mit OpenID

Insbesondere die Nachteile der Usability und des Datenschutzes der im vorherigen Abschnitt beschriebenen föderativen Verfahren werden bei den neu

entwickelten benutzerzentrierten Verfahren adressiert. Die Zentrierung auf den Benutzer ist dabei der nächste konsequente Schritt in Bezug auf die in Abbildung 1 gezeigte Dezentralisierung. Häufig wird in diesem Zusammenhang auch von „Identity 2.0“ oder „user-centric identity“ gesprochen [25].

Ähnlich wie bei der föderativen Authentifizierung werden bei der benutzerzentrierten Variante ebenfalls zwei beteiligte Parteien unterschieden. Zum einen der Provider (vergleichbar mit dem Identity Provider bei SAML), der die Identitäten der Benutzer lokal verwaltet. Zum anderen der Consumer (vergleichbar mit dem Service Provider bei SAML), der die eigentliche Ressource vorhält und vom Provider ausgestellte beglaubigte Authentifizierungs- und Autorisierungsinformationen konsumiert. Der im Shibboleth-Beispiel in Abbildung 2 gezeigte Discovery Service entfällt jedoch zu Gunsten der Usability. Der Benutzer wählt seine Identität (ID) selbst aus und übermittelt diese direkt beim Zugriff auf die Ressource an den Consumer. Als ID wird hierbei z. B. eine E-Mail-Adresse oder ein URL verwendet (z. B. http://mein-name.myopenid.com oder http://muster.xyz.mpg.de). Aufgrund des Aufbaus als URL oder E-Mail Adresse ist die ID global eindeutig (nicht nur auf eine Föderation beschränkt) und ubiquitär nutzbar. Anhand der ID kann der Cosumer (basierend auf der Domain) eigenständig den zuständigen Provider ermitteln. In Bezug auf die ID wird bei benutzerzentrierten Verfahren auch häufig von sog. Information Cards gesprochen. Information Cards (kurz: I-Cards) [26] können mit Visitenkarten verglichen werden. Benutzer, die mehreren Unternehmen angehören, können unterschiedliche Visitenkarten besitzen und verwenden. Dies adressiert auch die im vorherigen Abschnitt genannte Problematik der Zugehörigkeit einzelner Benutzer zu mehreren Föderationen. Um Information Cards zu verwenden, sind jedoch derzeit Erweiterungen erforderlich, um im Web-Browser die entsprechende Karte auszuwählen. Eine I-Card kann unterschiedliche Vertraulichkeitsstufen abbilden. Benutzer können sich selbst (self-signed) eine I-Card ausstellen, diese von einem vertrauenswürdigen Dritten (z. B. IdP) signieren lassen (managed) oder durch andere Benutzer bestätigen lassen (social networking). Bei der Verwendung der Karte können die Benutzer entscheiden, welche Informationen sie an den Consumer übermitteln wollen oder diese ändern (vgl. z. B. Entfernen einer Telefonnummer). Dies ermöglicht die Selbstbestimmung über die Identität und damit verbundene Daten auf der Seite der Nutzer und erhöht den Datenschutz gegenüber föderativen Verfahren.

Aktuell existieren unterschiedliche Implementierungen für benutzerzentrierte IdM-Verfahren. Seit 2008 haben sich einige große Unternehmen (als Provider: Google, IBM, Microsoft, Verisign und Yahoo!) für die Unterstüt-

zung des OpenID-Standards entschieden. Damit entwickelt sich OpenID derzeit zu einem de facto Standard unter den benutzerzentrierten IdM-Lösungen. Daneben besitzt noch der CardSpace-Standard von Microsoft durch die Integration in Windows Vista ein großes Potenzial, der auch im higgins-Projekt verwendet wird.

4.1 OpenID 2.0

Die Abbildung 3 zeigt den Ablauf einer benutzerzentrierten Anmeldung an einem OpenID-2.0-Consumer und -Provider. Dabei gibt der Benutzer beim Login im Consumer seine E-Mail-Adresse oder eine URL an. Anhand der Domain der Adresse kann der Consumer den zuständigen Provider ermitteln, der daraufhin eine XRDS-Nachricht [27] an den Consumer sendet, die die Schnittstelle für die Authentifizierung übermittelt. An diese richtet der Consumer anschließend die Authentifizierungsanfrage. Anschließend muss sich der Benutzer erfolgreich am Provider authentifizieren. Ist dies erfolgt, sendet der Provider eine beglaubigte persistente ID sowie Attribute des Benutzers an den Consumer, der basierend darauf den Zugriff auf die vom Benutzer gewünschte Ressource gewähren kann.

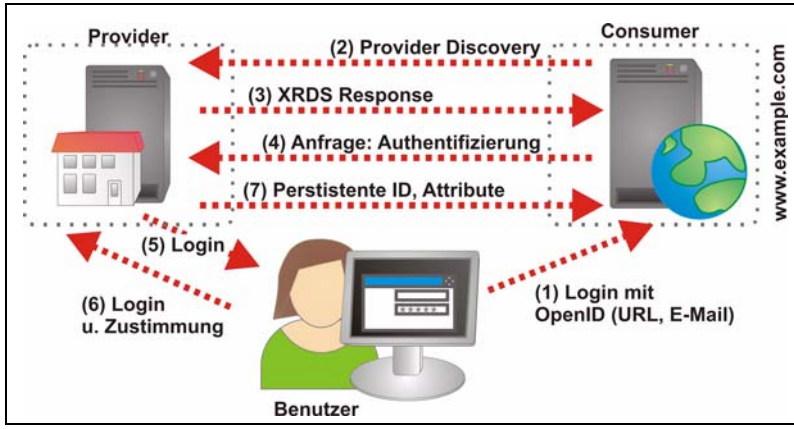


Abb. 3: Benutzerzentrierte Authentifizierung am Beispiel von OpenID

In den alternativen benutzerzentrierten Verfahren sowie Erweiterungen für den OpenID-Standard sind darüber hinaus weitere Funktionen implementiert. Beispielsweise sind unterschiedliche Identitäten des Benutzers möglich (vgl. Personas bei sxip [16]) oder digitale Signaturen für einzelne Attribute (Trusted Relying-Parties bei sxip und Card Space [14]).

4.2 Grenzen von OpenID

OpenID bietet insbesondere in Bezug auf die Discovery des Providers eine weitaus bessere Usability als SAML-basierte Verfahren. Bei benutzerzentrierten Verfahren, die eine Selektion der anhand der I-Card übermittelten Daten erlauben, ist zudem der Datenschutz deutlich erhöht. Allerdings erfordert diese Selektion derzeit (teilweise proprietäre) Erweiterungen für den Web-Browser. Auch die Übermittlung der Attribute selbst ist derzeit nur eine Erweiterung für den OpenID-Standard. Neben der Verwendung von I-Cards ist auch die bei OpenID verwendete ID nicht standardisiert. Während in der Regel URLs verwendet werden, setzen neue Implementierungen (Google) auf die E-Mail Adresse, wodurch einerseits die Usability weiter erhöht wird, aber andererseits eine abweichende Auslegung des Standards erfolgt, die ggf. nicht von allen Consumern unterstützt wird.

Darüber hinaus ist OpenID im Vergleich zu den SAML-basierten Verfahren noch ein relativ junger Standard, der noch einige Sicherheitslücken aufweist [28]. Beispielsweise können Phishing-Attacken erfolgen, sofern der Benutzer ohne HTTPS unbemerkt auf einen gefälschten Provider umgeleitet wird. Replay-Attacken und Man-in-the-Middle-Angriffe sind durchführbar, da im Standard keine wechselseitige Authentifizierung der Parteien (nur Diffie-Hellman-Schlüsselaustausch) definiert wird. Weitere Probleme bilden klassische Web-Sicherheitsprobleme wie Cross-Site-Scripting (XSS) und Cross-Site-Request-Forgeries (CSRF) [28].

Weitaus entscheidender ist der Nachteil der Bindung an einen konkreten Provider, der durch den Vorteil der global eindeutigen ID in Kauf genommen wird. Erhält ein Benutzer z. B. eine OpenID von einem bestimmten Provider und nutzt diese bei verschiedenen Consumern, so ist er von der Verfügbarkeit seiner ID beim Provider abhängig. Erhebt der Provider Kosten für die Verwendung der ID, so ist der Benutzer abhängig und muss zahlen, um die Consumer, bei denen er diese OpenID verwendet, und seine Daten weiterhin nutzen zu können. Außerdem ist der Provider in der Lage, Nutzungsprofile über seine Anwender beim Zugriff auf unterschiedliche Consumer zu erheben. Eine Lösung hierfür bildet der ursprüngliche Ansatz von OpenID als ID für die eigene Web-Seite bzw. URL (z. B. als Authentifizierung für Kommentare in Blogs). Durch diese Delegation können OpenID-Provider innerhalb der Domain der Heimat-Organisation betrieben werden. Allerdings bietet OpenID hierfür im Vergleich zur Föderation bei SAML keine Verfahren, um eine gemeinsame Vertrauensbasis über unterschiedliche Domains bzw. Organisationen hinweg zu ermöglichen.

5. Fazit und Ausblick

Benutzerzentrierte Authentifizierungsverfahren sind in Bezug auf die vereinfachte Usability und Discovery ideal für die Anwender. Die im vorherigen Abschnitt angesprochenen Sicherheitsprobleme werden aktuell gelöst bzw. werden in neueren Versionen von OpenID adressiert. Auch Erweiterungen für die Auswahl der Attribute (erhöhter Datenschutz) sowie die Übermittlung der Attribute werden von der OpenID-Foundation als Extensions standardisiert. Die Unterstützung durch Branchengrößen wie Google und Yahoo! für den OpenID-Standard sorgt zusätzlich für dessen Akzeptanz und Verbreitung. Allerdings bieten fast alle diese Unternehmen derzeit nur OpenID Provider für deren eigene Benutzer, nicht jedoch Consumer für ihre eigenen Dienste an. Besitzer einer Google-OpenID können beispielsweise keine Dienste von Yahoo! nutzen und umgekehrt. Die Benutzer benötigen daher nach wie vor unterschiedliche OpenIDs bzw. Benutzerkonten, um alle OpenID-Consumer verwenden zu können. Interessant ist die Unterstützung von OpenID durch die großen Unternehmen daher momentan nur für kleinere Firmen (z. B. Startups), die schnell eine große Benutzeranzahl erreichen wollen.

OpenID und SAML lösen gleiche Probleme und weisen individuelle Vor- und Nachteile auf. SAML und insbesondere dessen Implementierung Shibboleth sind derzeit der de-facto-Standard für wissenschaftliche Anwendungen wie E-Learning, den Zugriff auf Verlage oder GridShib (vgl. z. B. DFN-AAI [9], SWITCHaai [29], InCommon [30] oder FEIDE [31]). Für die MPG-AAI befindet sich eine Erweiterung für Shibboleth in der Entwicklung, die eine Anmeldung unter Verwendung der E-Mail-Adresse sowie damit verbunden eine Erhöhung der Usability und des Datenschutzes implementiert. Dies würde auch die Discovery für die Benutzung unterschiedlicher Föderationen erleichtern. Als Ideallösung kann in Bezug auf die konkurrierenden Verfahren SAML und OpenID deren Integration angesehen werden. Beispielsweise wäre eine Anmeldung mittels OpenID oder I-Card an einem Shibboleth-IdP denkbar. Teilweise stehen diese Erweiterungen auch schon in der langfristigen Planung auf den Roadmaps des Shibboleth-Projektes.

6. Referenzen

[1] SAML 2.0 Specifications: http://saml.xml.org/saml-specifications#samlv20.

[2] OpenID Specifications: http://openid.net/developers/specs.

[3] MPG Authentication and Authorization Infrastructure: https://aai.mpg.de.

[4] Windley, P. J.: Digital Identity, O'Reilly, 2005.

[5] Eckert, C.: IT-Sicherheit: Konzepte – Verfahren – Protokolle, Oldenbourg, 2004.

[6] Rieger, S.: Identity Management bei der GWDG, in Gartmann, C.; Jähnke, J.: GWDG-Bericht Nr. 70 „22. DV-Treffen der Max-Planck-Institute", 2006.

[7] Kerberos: http://web.mit.edu/kerberos.

[8] Rieger, S.: PKI-Leistungen der GWDG, in Gartmann, C.; Jähnke, J.: GWDG-Bericht Nr. 67 „21. DV-Treffen der Max-Planck-Institute", 2005.

[9] DFN-AAI - Authentifikation Autorisierungs Infrastruktur: https://www.aai.dfn.de.

[10] Shibboleth: http://shibboleth.internet2.edu.

[11] simpleSAMLphp: http://rnd.feide.no/simplesamlphp.

[12] Active Directory Federation Services: http://technet.microsoft.com/de-de/library/cc736690%28WS.10%29.aspx.

[13] Liberty Alliance Specifications: http://www.projectliberty.org/specifications__1.

[14] Introducing Windows CardSpace: http://msdn.microsoft.com/en-us/library/aa480189.aspx.

[15] OAuth: http://oauth.net.

[16] sxip Identity: http://www.sxip.com.

[17] higgins-Project: http://www.eclipse.org/higgins.

[18] eduPerson-Schema: http://middleware.internet2.edu/eduperson.

[19] DFN-PKI: http://www.pki.dfn.de.

[20] Kristol, D.; Montulli, L.: HTTP State Management Mechanism – RFC 2965, ftp://ftp.rfc-editor.org/in-notes/rfc2965.txt.

[21] eduGAIN: http://www.edugain.org.

[22] GridShib: http://gridshib.globus.org.

[23] Rieger, S.: Dezentrales Identity Management für Web- und Desktop-Anwendungen, in Müller, P.; Neumair, B.; Dreo Rodosek, G.: Lecture Notes in Informatics „1. DFN-Forum Kommunikationstechnologien“, Bonner Köllen Verlag, 2008.

[24] SWITCH AAI - uApprove: http://www.switch.ch/aai/support/tools/uApprove.html.

[25] Identity 2.0: http://identity20.com.

[26] Information Card Foundation: http://informationcard.net.

[27] Extensible Resource Identifier (XRI) and Extensible Resource Description (XRDS): http://docs.oasis-open.org/xri/2.0/specs/xri-resolution-V2.0.html.

[28] Wysopal, C.; Eng, C.: Static Detection of Application Backdoors, Blackhat 2007, https://www.blackhat.com/presentations/bh-usa-07/Wysopal_and_Eng/Whitepaper/bh-usa-07-wysopal_and_eng-WP.pdf.

[29] SWITCHaai Federation: http://www.switch.ch/aai.

[30] InCommon Federation: http://www.incommonfederation.org.

[31] Feide Federation: http://feide.no.

IT-Management mit Hilfe von Best-Practice-Referenzmodellen

Stefanie Alter

IT-Governance-Practice-Network, Frankfurt School of Finance and Management, Frankfurt

Kurzfassung

Führungsaufgaben der IT werden sowohl durch die Wissenschaft als auch durch praxisorientierte Institutionen, wie bspw. das IT Governance Institute (ITGI) oder den Berufsverband ISACA (Information Systems Audit and Control Association) adressiert und jüngst vermehrt diskutiert. Ergebnis dieses Prozesses sind einerseits wissenschaftlich etablierte Modelle des Informationsmanagements (IM) und andererseits praxisgeleitete, als „Best Practice“ entwickelte Referenzmodelle wie bspw. COBIT (Control Objectives for Information and related Technology) oder ITIL (IT Infrastructure Library). Diese Referenzmodelle haben eine tiefe Durchdringung in der Praxis und gewinnen daher auch zunehmend Beachtung in der Wissenschaft. Ziel dieses Beitrag ist es daher, die beiden gängigsten Modelle (COBIT und ITIL) vor dem Hintergrund des IT-Managements vorzustellen.

1. Führungsaufgabe der IT

In Unternehmen wird von der Informationstechnologie (IT) verstärkt gefordert, dass sie aktiver einen Wertbeitrag zu leisten habe. Dies bedeutet, von ihr wird zunehmend verlangt, flexibler, direkter und messbarer zum geschäftlichen Erfolg des Unternehmens beizutragen [KÖ06]. Damit ist die IT weitgehend der Möglichkeiten beraubt, sich als – bisweilen technikorientierter – interner Dienstleister einer Wirtschaftlichkeitsdiskussion entziehen zu können bzw. sich auf Kostengesichtspunkte zu beschränken. Neben diesem geschäftsgetriebenen Veränderungsdruck, der als Business-Pull bezeichnet werden kann, lässt sich eine technologieinduzierte Veränderung der IT feststellen. Diese als Technology-Push bezeichneten gestiegenen technischen Möglichkeiten erfordern unter anderem ein hohes Maß an Flexibilität und Schnelligkeit der IT.

Abgesehen von diesen veränderten Anforderungen hat sich auch der Umgang mit der Unternehmensressource Information selbst verändert. Gestiegener Umfang und wachsende Bedeutung haben dazu geführt, dass Information zunehmend einer aktiven Steuerung und Leitung bedarf. Nicht nur die Unterversorgung mit Information, sondern immer häufiger die Bewältigung der Informationsflut ist die Herausforderung. Der gestiegene Stellenwert zeigt sich auch darin, dass die Etablierung der Informationsfunktion auf Vorstandsebene, in Gestalt des CIO, zunimmt. Bislang entscheiden jedoch häufig die intuitiven Fähigkeiten des CIO darüber, wie erfolgreich mit den Herausforderungen der IT umgegangen wird [JG07]. Dies ist u. a. auf eine bislang unzureichende Unterstützung durch geeignete Methoden und Techniken zurückzuführen. So fehlen bislang insbesondere ganzheitliche wissenschaftliche Modelle und Methoden, die das Management d. h. die Führungsaufgabe, unterstützen. Empirische Untersuchungen zeigen, dass gerade ein effektives und effizientes Management des Technologieeinsatzes einen höheren Beitrag der IT zum Erfolg des Unternehmens bewirkt [RS05, TK98].

Im Gegensatz zur Wissenschaft hat die Praxis frühzeitig die Möglichkeiten des konsequenten Managements der IT erkannt und die Nachfrage nach Konzepten für die Erfüllung dieser Führungsaufgabe ist dementsprechend hoch [ZBP06]. Dieser Nachfrage wurden insbesondere Unternehmensberatungen aber auch Berufsverbände und andere Institutionen gerecht, indem sie Ansammlungen von Wissen und „Best Practices“ zu Referenzmodellen konsolidiert haben. Einige dieser Best-Practice-Ansätze haben einen hohen Bekanntheits- und Verbreitungsgrad erlangt und entwickeln sich durch einen kontinuierlichen Prozess aus Veröffentlichungen, Anwendungen und Verbes-

serungen weiter. Ziel dieses Beitrages ist es, Best-Practice-Ansätze aus Sicht des Informationsmanagements zu beurteilen. Es wird der Frage nachgegangen, wie die genannten Modelle in den wissenschaftlichen Kontext einzuordnen sind und ob sie aus wissenschaftlicher Sicht eine methodische Unterstützung der Führungsaufgabe des Informationsmanagements leisten können.

2. Informationsmanagement als wissenschaftliche Disziplin

In der Wissenschaftslandschaft ist die Führungsaufgabe in der IT eine Domäne des Informationsmanagements. Das Informationsmanagement ist eine zentrale, jedoch lange Zeit eher stiefmütterlich behandelte Teil-Disziplin der Wirtschaftsinformatik.[1] Es ist Einflüssen verschiedenster Forschungsrichtungen ausgesetzt und sein Gegenstandsbereich ist, ähnlich dem anderer Sozialwissenschaften, nicht eindeutig definiert. Jedoch ist es seinen Wurzeln (bspw. den Bibliotheks- und Informationswissenschaften) ebenso entwachsen wie der reinen Entwicklung computergestützter Informations- und Kommunikationssystemen [TK02].

Wird das Informationsmanagement auch als Führungsaufgabe verstanden und damit klar vom technischen Verständnis abgehoben, stellt sich die Frage, welche Konzepte, Aufgaben und Methoden den Herausforderungen strategischer Natur gerecht werden.

In diesem Kapitel wird zunächst kurz der Stand der Forschung des Informationsmanagements skizziert. Hierzu werden im folgenden Abschnitt 2.1 *Konzepte* des Informationsmanagements unterschieden und systematisiert. Üblicherweise beschreiben die Konzepte verschiedene *Aufgaben* sowie *Methoden* zu ihrer Unterstützung. Aufgaben und Methoden sind Gegenstand des nachfolgenden Abschnitts 2.2.

2.1 Konzepte des Informationsmanagements

In einer Reihe etablierter Monographien sind in der Vergangenheit verschiedene Konzepte des Informationsmanagements entwickelt worden (vgl. u. a. [He99, HL05, Kr05, LHM95, Sc98, VG01]). Hierbei kann man eine zeitliche Entwicklung des IM-Begriffs beobachten. Diese lässt eine allmähliche Ausweitung und Verschiebung des Gegenstandsbereiches erkennen: So wandelte sich der dominierende Aspekt der IM-Definitionen von „Entwicklung

1. Indizien hierfür mögen sein, dass es keine aktive Fachgruppe im Fachbereich 5 der GI gibt und dass auf den vergangenen großen WI-Konferenzen das Informationsmanagement stets nur am Rande behandelt wurde.

und Betrieb von IV-Systemen“ (bspw. [Ös89] mit Abstrichen auch [Schm96]) über die „Informationsversorgung“ [Hü96] hin zu einem umfassenden Begriffsverständnis des Informationsmanagements nach [Kr05, ÖBH92, VG01 oder HL05]. Beim umfassenden Begriffsverständnis ist die Systementwicklung i. e. S. von untergeordneter Bedeutung. Im Mittelpunkt steht dagegen die „wirtschaftliche (effiziente) Planung, Beschaffung, Verarbeitung, Distribution und Allokation von Informationen als Ressource zur Vorbereitung und Unterstützung von Entscheidungen … sowie die Gestaltung der dazu erforderlichen Rahmenbedingungen“ [VG01, S. 70]. Im Folgenden sollen verschiedene Systematisierungen von IT-Konzepten dargestellt werden, da diese den Gegenstandsbereich und dessen Wandel anschaulich werden lassen.

Peterhans systematisiert in [LHM95] die „Theorien des IM“ nach dem Erkenntnisobjekt. Hieraus resultiert eine Unterscheidung in eine *individuelle*, eine *kollektive*, eine *organisatorische* und eine *interorganisationale* Perspektive. Diese Systematisierung nimmt keine Strukturierung vorhandener Konzepte anhand der vorgesehenen Aufgaben und/oder Methoden vor und ist daher für die hier verfolgte Zielsetzung kaum zu verwenden.

Teubner diskutiert den State-of-the-Art des Informationsmanagements und wählt eine – zuletzt historisch motivierte – Systematisierung in IM als Management der *Informationsressourcen*, als Management der *Informationssysteme* und als Management der *Informationsfunktion*. Nach einer kritischen Analyse verschiedener Ansätze, die er in diese Systematik einordnet, formuliert er drei Erweiterungsvorschläge: Das „ganzheitliche Informationsmanagement“, ein „integriertes Informationsmanagement“ und „unternehmerisches Informationsmanagement“. Beim integrierten Informationsmanagement diskutiert er – aufbauend auf [Kr05] – die „Führungsaufgabe des Informationsmanagements“.

[Kr05] selbst unterscheidet fünf Ansätze des Informationsmanagements: problemorientierte, aufgabenorientierte und prozessorientierte Ansätze sowie Ebenenmodelle und Architekturmodelle. Ergänzen ließen sich wertschöpfungsorientierte Konzepte wie das IM-Verständnis von [ZBP06], welches das aus der Logistik stammende SCOR-Modell verwendet. Dieses Modell wird auch als „Gesamtmodell des integrierten Informationsmanagements“ bezeichnet. Von einer ähnlichen Autorengruppe des IWI (St. Gallen) stammt das *produktorientierte Informationsmanagement* [ZB03]. Hierbei werden „IT-Produkte“ als Basis der Zusammenarbeit zwischen IT und Geschäftsbereichen vorgeschlagen und Sichtweisen, Aufgaben und Verantwortlichkeiten eines entsprechenden Informationsmanagements beschrie-

ben. Dieses Konzept kann als Vorläufer des „Gesamtmodell des integrierten IM“ gewertet werden.

Als besonders etabliert könnten nach Ansicht der Verfasser solche Informationsmanagementkonzepte angesehen werden, die in Ebenenmodellen die Nähe zur technischen Implementierung oder Managementebenen heranziehen (vgl. Tabelle 1). Diese werden im Folgenden herangezogen, um Best-Practice-Referenzmodelle einzuordnen.

Krcmar [Kr01]	**Voß/ Gutenschwager [VG01]**	**Heinrich/ Lehnert [HL05]**
Informationswirtschaft	Informationseinsatz	Strategische Ebene
Informationssysteme	IKS	Administrative Ebene
Informations- und Kommunikationstechnik	IK-Infrastruktur	Operative Ebene
+ Ebenenübergreifende Führungsaufgaben		

Tabelle 1: Übersicht der Informationsmanagementkonzepte

[VG01] merken kritisch die vorherrschende Technikorientierung der Mehrzahl der IM-Konzepte an. Gleichwohl wird jedoch bei Betrachtung der Historie – die sich bspw. in der Terminologie und Schwerpunktsetzung der Konzepte widerspiegelt – deutlich, dass vermehrt auch betriebswirtschaftliche Aspekte und prozessuale sowie institutionelle Gesichtspunkte hinterfragt werden, wenn sie auch noch nicht in befriedigendem Maße beantwortet sind. Eine umfassende, explizite und integrierte Thematisierung der Führungsaufgabe bzw. des Leitungshandeln des Informationsmanagements findet sich dagegen seltener. Bei [VG01] finden sich kurze Ausführungen zum DV- und Infrastrukturmanagement sowie zum Controlling der Informationsverarbeitung, die als übergreifend aufgefasst werden können. [Kr01] hingegen räumt Governance-, Strategie-, Personal- und Controllingaspekten breiten Raum ein. [ZBP06] sehen als einen Bestandteil ihres integrierten Informationsmanagements den Baustein „Govern“, der – in Anlehnung an COBIT (s. u.) –

für strategische Ausrichtung, Value Delivery, Risiko- und Ressourcenmanagement sowie Controlling zuständig ist.

2.2 Aufgaben und Methoden des Informationsmanagements

Die oben diskutierten Konzepte des Informationsmanagements bestimmen durch ihre Grundstruktur (in Tabelle die Ebeneneinteilung) über die Anordnung von Aktivitäten, Aufgaben oder Teilprozessen und deren Methoden und Techniken. Die Begriffe Methoden, Werkzeuge, Techniken werden jedoch in der Wirtschaftsinformatik allgemein – und so auch im Informationsmanagement – äußerst unterschiedlich aufgefasst. So beinhaltet eine Methode nach dem St. Gallener Ansatz des Methoden Engineering bspw. die Komponenten Metamodell, Technik, Ergebnis, Rolle und Aktivität, während [HL05] eine Methode als ein auf einem System aus Regeln aufgebautes Problemlösungsverfahren beschreibt (z. B. Algorithmus). Auch werden hier die Begriffe Methoden und Techniken synonym verwendet. Die Bandbreite der verschiedenen Verständnismöglichkeiten erweitert [Br96, Br99], indem er Prinzipien zu den Methodenkomponenten zählt. Sie finden als „way of thinking“ Eingang in das Methodenverständnis.

[Kr05] clustert die Aufgaben des Informationsmanagements in die Bereiche Management der Informationswirtschaft, Management der Informationssysteme, Management der Informations- und Kommunikationstechnik und in Führungsaufgaben des Informationsmanagements. Dieser groben Gliederung folgen detaillierte Beschreibungen der einzelnen Aufgaben und eine Zuordnung von Methoden zur Realisierung der jeweiligen Aufgaben (Jedoch expliziert er sein Methodenverständnis nicht). Andere Autoren wie bspw. [HL05] oder [Sc98] unterteilen die Aufgaben des IM mithilfe der Managementebenen und weisen den strategischen, administrativen und operativen Aufgaben des IM jeweils Methoden zu. Hier wird allerdings global zugeordnet, d. h. Methoden und Techniken (hier synonym) des Informationsmanagements werden den genannten Ebenen insgesamt zugeordnet und nicht einer einzelnen Aufgabe (vgl. Tabelle 2).

Strategische Ebene	
Aufgaben	**Methoden**
Situationsanalyse	Benutzerbeteiligung
Zielplanung	Szenariotechnik
Strategieentwicklung	Strategieentwicklung
Maßnahmenplanung	Portfolioanalyse
Qualitätsmanagement	Erfolgsfaktorenanalyse
Technologiemanagement	Korrelationsanalyse
Controlling	Kennzahlensysteme
Revision	Wirtschaftlichkeitsanalyse
	Nutzwertanalyse
	Evaluierungsmethoden
Administrative Ebene	
Projektmanagement	Geschäftsprozessmanagement
Personalmanagement	Wissensmanagement
Datenmanagement	Wertanalyse
Lebenszyklusmanagement	Aufwandsschätzung
Geschäftsprozessmanagement	Kosten- und Leistungsrechnung
Wissensmanagement	Benchmarking
Vertragsmanagement	Checklisten
Sicherheitsmanagement	Risikoanalyse
Katastrophenmanagement	Computer-Versicherungen
	Fehlerbaumanalyse
	Qualitätsmodelle
Operative Ebene	
Produktionsmanagement	Hardware- Software-Monitoring
Problemmanagement	Abrechnungssysteme
Benutzerservice	Service Level Agreements

Tabelle 2: Aufgaben und Methoden des IM nach Heinrich

Als Zwischenfazit kann man festhalten, dass dem Informationsmanagement eine zentrale Bedeutung als anwender- und unternehmensorientierte Koordinations- und Gestaltungsfunktion zugeschrieben wird. Gleichwohl wird jedoch auch deutlich, dass sowohl der Begriff Informationsmanagement als auch seine Aufgaben, Methoden und Techniken in der Wissenschaft nicht besonders klar umrissen sind. Aufgaben sind häufig auf den Kontinuen zwi-

schen „Business“/Informationsnutzung und Technik bzw. strategischem und operativem Management angesiedelt. Sie dienen jeweils dazu, die Brücke zwischen den Eckpunkten zu schlagen. Die diesen Aufgaben mehr oder weniger direkt zugeordneten Methoden und Techniken weisen dagegen eine große Heterogenität und eine geringe Integration auf. So wird bspw. die „Benutzerbeteiligung“ als Methode eingeordnet – in der Systementwicklung wäre sie dagegen als Prinzip klassifiziert. „Geschäftsprozessmanagement“ ist ebenfalls eher ein Organisationskonzept und scheint auf anderer Ebene zu sein als die ebenfalls aufgeführten „Rechenverfahren“.

3. Best-Practice-Referenzmodelle

Nicht zuletzt auch deshalb, weil das Thema IT-Management in der Wissenschaft eher als Thema „der zweiten Reihe“ gelten kann, wurden in der vergangenen Dekade eine Reihe von offenen bzw. herstellerunabhängigen (bspw. ITIL und COBIT) und herstellerspezifischen Referenzmodellen entwickelt (Microsoft Operations Framework (MOF), das IT-Service-Management (ITSM) von Hewlett-Packard oder das IBM IT Process Model (ITPM)). Diese Referenzmodelle, die auch unter dem sich entwickelnden Thema „IT-Governance“ subsumiert werden, beschreiben Ziele, Aufgaben, organisatorische Aspekte und konkrete Ergebnisse der IT-Steuerung und Kontrolle, die zur Unterstützung für das Management der IT herangezogen werden können [JG06, JG07]. Im Folgenden werden ausschließlich die herstellerunabhängigen Modelle COBIT und ITIL betrachtet.

Die offenen und herstellerunabhängigen Modelle lassen sich treffend als „von der Praxis – für die Praxis“ beschreiben. Interessant erscheint die Entstehung von Best-Practice-Modellen: Industrievertreter und ggf. Wissenschaftler verdichten ihr Wissen mit dem Ziel, allgemein akzeptierbare Methoden, Prozesse, Eigenschaften usw. zu definieren. Wesentlich ist die Konsolidierung von Wissen aus Erfahrung. Obwohl sich an der Entwicklung der o. g. Modelle wie COBIT und ITIL vereinzelt auch Wissenschaftler beteiligen, sind jedoch vor allem Praktiker Mitglieder der konstituierenden Experten-Gremien. Auch fehlt bislang eine breite wissenschaftliche Diskussion dieser Modelle. Eine intensive Auseinandersetzung erscheint jedoch zweckmäßig, nicht nur da sie eine intensive Verbreitung in der Praxis gefunden haben, sondern auch, da sie eine große Menge an konsolidiertem (Erfahrungs-)Wissen enthalten.

Im Folgenden wird das Referenzmodell COBIT (Control Objectives for Information and related Technology) in seiner aktuellen Version beschrieben, soweit dies für die hier gewählte Fragestellung zielführend ist. Eingegangen wird auch auf die IT Infrastructure Library (ITIL), die sich in ihrer

neuesten Version in einigen Aspekten COBIT deutlich angenähert hat [GR07].[2]

3.1 Control Objectives for Information and related Technology (COBIT)

Im Kern beschreibt COBIT ein generisches Prozessmodell, welches die relevanten Prozesse und Aktivitäten, die man gemäß Best-Practice-Vorstellungen in einer IT-Abteilung oder -Organisation finden sollte, definiert. Während frühere Versionen den Schwerpunkt auf Gesichtspunkte der Wirtschaftsprüfung (IT-Audits) legten, hat sich das COBIT-Referenzmodell unterdessen zu einer Ergänzung der Methoden des IT-Managements entwikkelt, das über das Audit hinaus eine Vielzahl betriebswirtschaftlicher Aspekte umfasst. In einer Makroperspektive werden die IT-Prozesse angeordnet, indem sie in vier so genannte Kontrollbereiche (Domänen) gruppiert werden, die sich an dem Lebenszyklus von Anwendungssystemen orientieren. Abbildung 1 zeigt die 34 Prozesse des COBIT-Frameworks innerhalb der Domänen:

- Plan and Organize,
- Aquire and Implement,
- Deliver and Support und
- Monitor and Evaluate.

Für jeden der 34 IT-Prozesse werden eine Vielzahl von Komponenten definiert, wie geschäftliche Anforderungen, Ziele, Schlüsselkontrollen und Metriken sowie Aktivitäten, betroffene Ressourcen, Verantwortlichkeiten etc.

2. [ITGI03b, ITGI07, OGC 2007a, OGC 2007b, OGC 2007c, OGC 2007d, OGC 2007e]

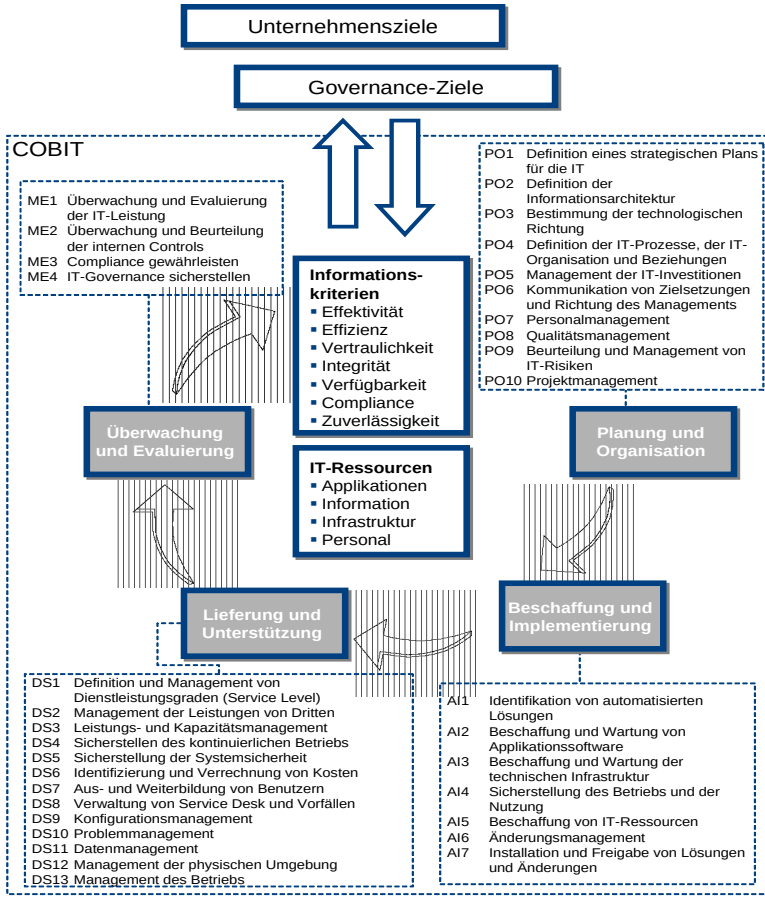


Abbildung 1: COBIT-Prozesse sortiert nach Domänen

Im Detail bedeutet dies, jeder der 34 IT-Prozesse produziert Ergebnisse, d. h. einen Output, welcher für die nachfolgenden Prozesse wiederum Input darstellen kann. Weiterhin besteht ein Prozess aus *Control Objectives* und beinhaltet *Aktivitäten*, die von *Rollen* ausgeführt werden. Das Rollenkonzept von COBIT kennt vier Arten von Rollenqualität: Responsible, Accountable, Consulted und Informed.[3] Diese sind nicht disjunkt, d. h ein Mitarbeiter

3. Abgebildet in sogenannten RACI-Charts

kann allen vier Rollen zugeordnet sein oder seine Rolle von Prozess zu Prozess differieren. Außerdem enthält das Rollenkonzept von COBIT zusätzlich eine Unterteilung nach Rolle in der hierarchischen Struktur des Unternehmens (IT-Leitung, Geschäftsführung etc.). Ob alle Rollen besetzt sein müssen und ob die Aufzählung vollständig ist, wird im Framework nicht diskutiert.

Jeder Prozess des Frameworks unterstützt Ziele, welche sich in *IT-Ziele*, *Prozessziele* und *Aktivitätsziele* aufteilen lassen. Diese Ziele stehen wiederum in Beziehung. So lösen IT-Ziele Prozessziele aus, die wiederum in Aktivitätszielen münden. Jedes Ziel wird mithilfe verschiedener *Metriken* gemessen. Außerdem erfüllt ein Prozess *Information Criteria*, diese können primär oder sekundär fokussiert sein. Die Information Criteria haben die Ausprägungen Effectiveness, Efficiency, Confidentiality, Availability, Compliance and Reliability. Weitere Bestandteile von COBIT sind ein *Reifegradmodell*, vier *Domänen* und *IT-Ressourcen*. Jeder Prozess kann mit Hilfe eines Reifegradmodells hinsichtlich seines Reifegrades beurteilt werden. Dies ist der Ausgangspunkt für eine kontinuierliche Verbesserung der Prozessreife und deren Kontrolle zum Beispiel durch Soll-Ist-Vergleiche. Jeder Prozess ist einer Domäne zugeordnet, welche nach dem Lebenszyklusprinzip angeordnet sind. Die Zuordnung erfolgt in die Domänen Plan and Organize, Acquire and Implement, Deliver and Support und Monitor and Evaluate. Um Ergebnisse zu produzieren, benötigt ein Prozess außerdem *IT-Ressourcen*. Jeder Prozess hat die Attribute Prozesskürzel und Prozessbeschreibung. Das Prozesskürzel identifiziert den Prozess eindeutig. Es besteht aus der Domänenabkürzung und einer fortlaufenden Nummer. Beispielsweise PO 4 für den 4. Prozess in der Domäne *Plan and Organize*.

Die *IT Governance Focus Areas* bilden die Bereiche Strategic Alignment, Value Delivery, Risk Management, Performance Measurement und Resource Management, welche primär oder sekundär durch einen oder mehrere Prozesse unterstützt werden.

Nach diesem allgemeinen Aufbau soll nun der Prozess AI 6 Change Management beispielhaft beschrieben werden. Der Prozess AI 6 ist der Domäne Acquire and Implement zugeordnet und beschreibt das Veränderungsmanagement. Der Prozess hat die folgenden fünf Control Objectives:

AI6.1 Standards und Verfahren für Changes

Erstelle formelle Change-Management-Verfahren, um in geregelter Weise alle Anfragen (inklusive Wartung und Patches) für Changes an Anwendungen, Verfahren, Prozessen, System- oder Serviceparametern sowie an Basisplattformen zu behandeln.

AI6.2 Bewertung von Auswirkungen, Priorisierung und Freigabe

Stelle sicher, dass alle Anfragen für Changes in einer strukturierten Art und Weise auf deren Auswirkungen auf die operativen Systeme und deren Funktionalität hin beurteilt werden. Diese Beurteilung sollte eine Kategorisierung und Priorisierung der Changes umfassen. Vor der Migration in die Produktion werden Changes durch die jeweiligen Stakeholder genehmigt.

AI6.3 Notfalls-Changes

Erstelle einen Prozess für die Definition, Aufnahme, Beurteilung und Genehmigung von Notfalls-Changes, die nicht dem bestehenden Change-Prozess folgen. Dokumentation und Tests sollten durchgeführt werden, auch nach der Implementierung des Notfalls-Changes.

AI6.4 Statusverfolgung und Berichterstattung

Erstelle ein Nachverfolgungs- und Reportingsystem, um die entsprechenden Stakeholder über den Status der Änderung an Anwendungen, Verfahren, Prozessen, System- oder Serviceparametern sowie an den Basisplattformen informiert zu halten.

AI6.5 Abschluss und Dokumentation von Changes

Sobald System-Changes umgesetzt sind, aktualisiere die betreffende System- und Benutzerdokumentation sowie die Verfahren entsprechend. Erstelle einen Review-Prozess, um die vollständige Umsetzung der Changes sicherzustellen.

Zusätzlich hat der Prozess AI 6 alle oben beschriebenen Elemente. D. h. Ziele (etwa „Festlegung und Kommunikation der Verfahren für Changes inklusive Notfalländerungen und -patches“ oder „Minimiere Fehler, die durch unvollständige Anfrage-Spezifikation hervorgerufen sind“), Metriken (bspw. „prozentualer Anteil der aufgezeichneten und mit automatisierten Tools verfolgten Änderungen“ oder „Nacharbeit an Anwendungen, die durch mangelhafte Spezifikation der Änderungen hervorgerufen ist“) sowie Verantwortlichkeiten u. v. m. COBIT bietet demnach einen möglichen Soll-Zustand und erleichtert das IT-Management, indem konkrete Vorschläge zur Prozessgestaltung, -ausführung und -kontrolle bereitgestellt werden.

3.2 IT Infrastructure Library (ITIL)

Die IT Infrastructure Library hat im Vergleich zu COBIT eine stärker operative Ausrichtung. Der Fokus liegt dabei auf den aktuellen und zukünftigen Herausforderungen für die IT im Allgemein und für das Servicemanagement

im Besonderen, wie z. B. Sourcing, Virtualisierung und die Notwendigkeit, IT stärker als bisher »als Geschäft zu betreiben«. Besonders seit der Veröffentlichung von ITIL V3 ist die Bereitstellung flexibler, dynamischer und erprobter Servicemanagementmethoden das Ziel des ITIL-Standards. Stärker als in der Vorgängerversion zeigt V3, wie ein (Wert-)Beitrag zu den Unternehmenszielen geleistet werden kann. ITIL V3 besteht aus fünf Büchern, die im Folgenden kurz vorgestellt werden sollen [GR07]. Abbildung 2 zeigt das Zusammenspiel der einzelnen ITIL-Bücher.

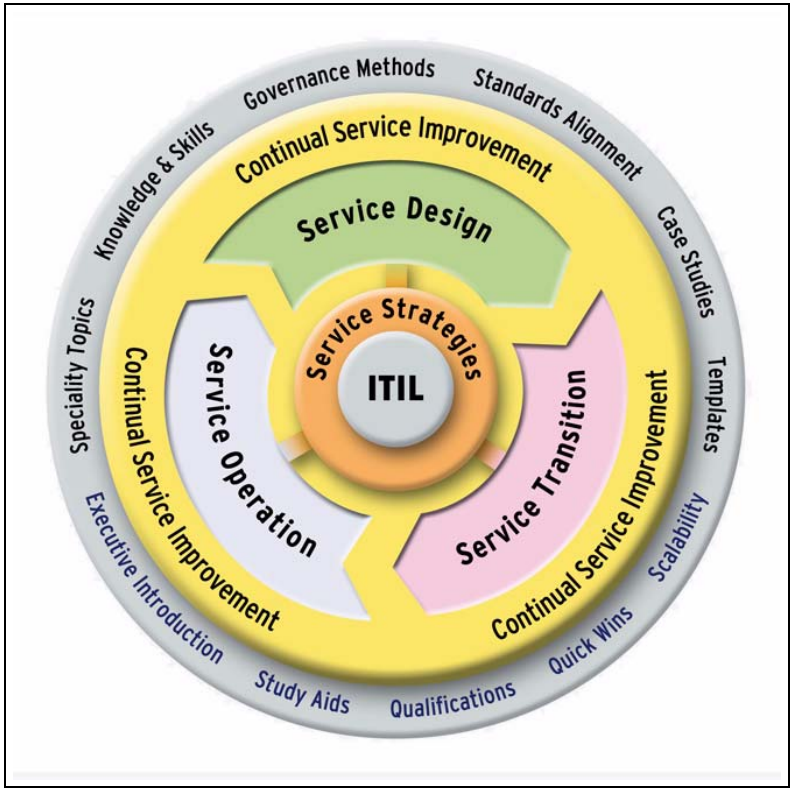


Abbildung 2: ITIL V3 (Quelle: [GR07])

Service Strategy [OGC 2007a]

Die Abstimmung zwischen dem Kerngeschäft und der IT-Abteilung eines Unternehmens wird durch unterschiedliche Sichtweisen, Ziele und Sprachwelten behindert. Zunächst geht es daher in dem Band Service Strategy um die Etablierung von strategischem Denken bei der Abstimmung zwischen

dem Kerngeschäft eines Unternehmens und seiner IT sowie um die Definition einer Strategie für das gesamte IT-Servicemanagement. Die Service Strategy steht daher im Zentrum des ITIL-Lebenszyklus. Beschrieben werden die Grundzüge eines effektiven IT-Servicemanagements sowie dessen Entwicklung und Integration in das Unternehmen. Dies beinhaltet neben der Festlegung des »Marktes« und der relevanten Kunden die Entwicklung eines abgestimmten Angebots und das Management der Nachfrage. Als unterstützende Methoden hierfür werden u. a. Finanzmanagement und Serviceportfoliomanagement dargestellt. Darüber hinaus wird die zentrale Rolle der Service Strategy und ihr Verhältnis zu den anderen Prozessen beschrieben. Wie in allen Bänden werden organisatorische Aspekte sowie Herauforderungen, Erfolgsfaktoren und Risiken diskutiert. Darüber hinaus wird insbesondere die strategische Bedeutung des Sevicemanagements betont.

Service Design [OGC 2007b]

Der Bereich Service Design hat eine wichtige Funktion bei der (lebens-) zyklischen Interpretation von Services. Neben dem Entwurf neuer wird auch die Weiterentwicklung bestehender Prozesse beschrieben. Der Band Service Design bietet daher Hilfestellung bei der Entwicklung und Gestaltung von Servicemanagementprozessen, die sicherstellen sollen, dass ein anforderungsgerechtes Serviceangebot bereitgestellt werden kann. Dies beinhaltet entsprechende IT-Prozesse, eine angemessene Dokumentation sowie eine Architektur und Richtlinien. Service Design ist ein iterativer Prozess, bei dem zunächst ein Entwurf des Service entwickelt wird, der in späteren Phasen des Lifecycles ausgebaut, getestet und in die Produktion überführt wird.

Service Transition [OGC 2007c]

Dieser Band betrachtet den Überführungsprozess eines IT-Service in das Geschäftsumfeld eines Unternehmens und die hierzu erforderlichen Fähigkeiten. Hierfür werden Methoden der unterbrechungsfreien Integration in das operative Geschäft beschrieben. Dies ist notwendig, da die Rechtzeitigkeit der Bereitstellung von Services sowie ihrer Effizienz und Sicherheit für das Zusammenspiel von IT und Kerngeschäft von entscheidender Bedeutung sein kann. Dieser Band beinhaltet außerdem Leistungsbewertung und -prognose für neue oder geänderte Services, die in den operativen Betrieb überführt werden, sowie die Ressourcenplanung und -steuerung hierfür. Des Weiteren beschäftigt sich Service Transition mit Risikoprognosen sowie Wartungsaufgaben bezüglich der durchgeführten Releases.

Service Operation [OGC 2007d]

Service Operation beinhaltet den operativen Teil des IT-Servicemanagements, bestehend aus der Abwicklung und Ausführung von Services. Service Operation liefert Lösungsansätze für die alltäglichen Aufgaben der IT-Organisation. Mithilfe der Angaben soll eine größere Effektivität und Effizienz bei der Lieferung von Services gewährleistet werden. Hierfür werden organisatorische Aspekte bezüglich der operativen Abwicklung sowie Richtlinien für z. B. Monitoring, Measurement, Reporting und Dokumentation beschrieben. Abschließend folgen technische Aspekte zur Abwicklung der alltäglichen Aufgaben einer IT-Organisation und eine Beschreibung des Implementierungsprozesses.

Continual Service Improvement [OGC 2007e]

Den äußeren Rand des ITIL-Lebenszyklus bildet der Prozess Continual Service Improvement (CSI). Beschrieben werden die Rahmenbedingungen für einen kontinuierlichen Verbesserungsprozess, welcher die bereits beschriebenen anderen Bände umfasst. Der Band gibt eine ausführliche Einführung in das Konzept von CSI, erläutert den durch CSI erhaltenen Mehrwert und beschreibt die gebräuchlichen Methoden und Techniken sowie deren Anwendung. Zu den wesentlichen Kernelementen gehören die Prozesse für das Qualitätsmanagement und das Changemanagement sowie die Verbesserung der Unternehmenskompetenzen (Capability Improvement).

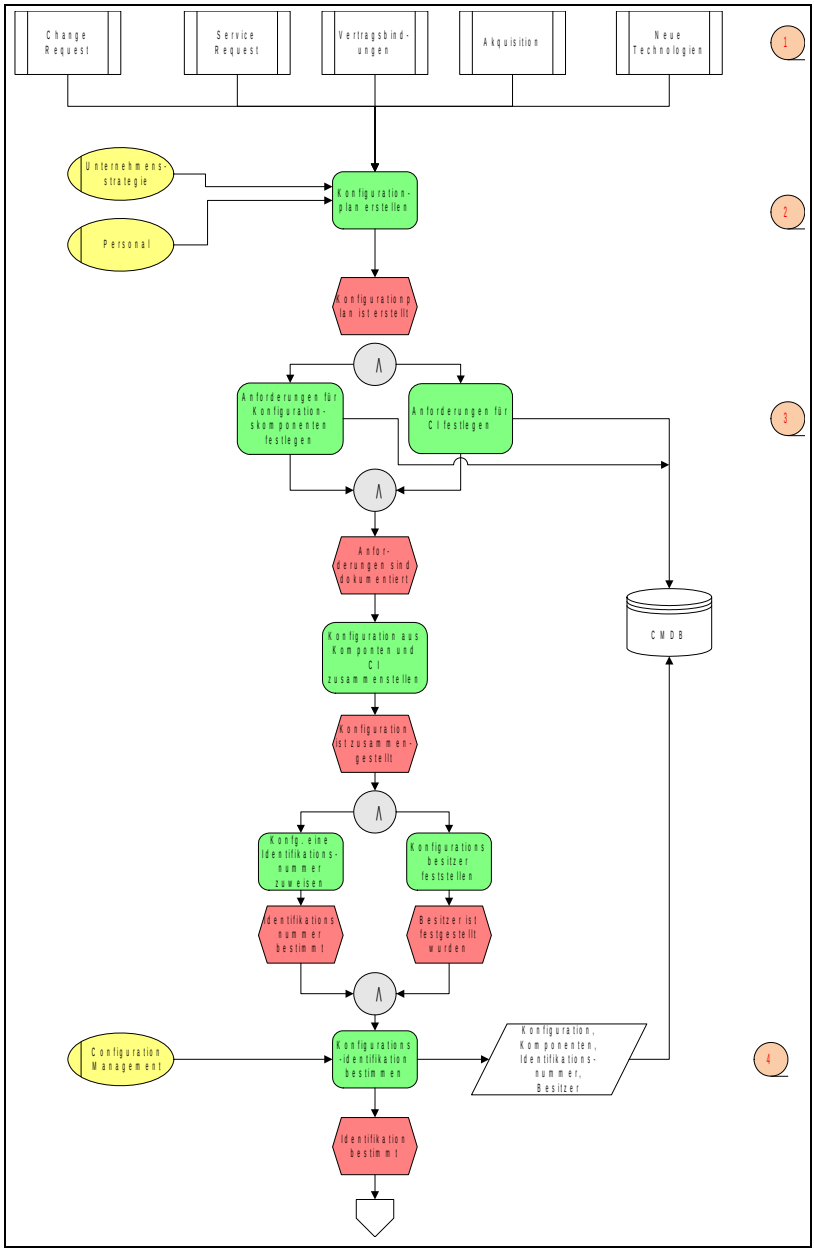


Abbildung 3: Der ITIL-Prozess Change Management

Abbildung 3 zeigt ein Ablaufdiagramm des Prozesses Change Management des ITIL-Standards. An diesem Beispiel, insbesondere im Vergleich zum COBIT-Prozess AI 6, wird deutlich, dass ITIL eine stärker operative Ausrichtung hat.

Sowohl COBIT als auch ITIL bieten demnach Möglichkeiten, das Management der IT zu unterstützen. Soll in einem Unternehmen die IT-Abteilung professionalisiert werden, sind neben den klassischen wissenschaftsgetriebenen Modellen praxisgetriebene Best-Practice-Modelle eine mögliche Bereicherung. Insbesondere der Blickwinkel der Modelle, der als „von der Praxis – für die Praxis“ bezeichnet werden kann, ist für eine alltägliche Verwendung vorteilhaft.

4. Zusammenfassung und Ausblick

Als Fazit wird festgehalten, dass die diskutierten Best-Practice-Referenzmodelle eine sinnvolle *Ergänzung* zu den bisherigen Systematiken und Konzepten für das Management der IT sind. Das in den Modellen konsolidierte Wissen erfahrener Praktiker, das induktive Vorgehen bei der Entwicklung und die Lebenszyklus- und Prozessorientierung sind gute Argumente für eine Verwendung von Best-Practice-Modellen. Weiterer Forschungsbedarf ergibt sich vor allem im Bereich Implementierungsunterstützung. So müssen Aspekte wie die unternehmensspezifische Adaption, die Priorisierung der einzuführenden Prozesse und auch die Folgen einer nur teilweisen Einführung analysiert werden.

Im Rahmen eines Verbund-Projekts (Forschungsförderung im Zuge der LOEWE-Initiative des Landes Hessen) wird daher bereits an der toolunterstützten Einführung von Referenzmodellen gearbeitet. In Zusammenarbeit mit mehreren Partnern soll ein Tool entstehen, das auf Basis semantischer Technologien die unternehmensspezifische Adaption, die Einführung und die Nutzung von Referenzmodellen erleichtert. Das Max-Planck-Institut für Herz- und Lungenforschung, Bad Nauheim, ist einer der Praxispartner des bis Oktober 2010 veranschlagten Projekts.

Literatur

[Br96] Brinkkemper, S.: Method engineering: engineering of information systems development methods and tools, In: Information and Software Technology, 38, 4, 1996, 275-280.

[Br99] Brinkkemper, S., et al.: Meta-modelling based assembly techniques for situational method engineering, In: Information Systems, 24, 3, 1999, 209-228.

[GR07] Goeken, M.; Reimann, B.: ITIL v3 - Alles neu macht der Mai?, In: IT-Governance - Zeitschrift des ISACA Germany Chapter, 1, 2, 2007.

[He99] Heinrich, L. J.: Informationsmanagement, Oldenbourg, München, 1999.

[HL05] Heinrich, L. J.; Lehner, F.: Informationsmanagement, Oldenbourg, München, Wien, 2005.

[Hü96] Hübner, H.: Informationsmanagement und strategische Unternehmensführung, Oldenbourg, München, Wien, 1996.

[ITGI03b] IT Governance Institute: COBIT Implementation Guide, o. O., 2003.

[ITGI07] IT Governance Institute: COBIT 4.1, o. O, 2007.

[JG06] Johannsen, W.; Goeken, M.: IT-Governance - neue Aufgaben des IT-Managements, In: HMD - Praxis Wirtschaftsinformatik, 250, 2006, 7-20.

[JG07] Johannsen, W.; Goeken, M.: Referenzmodelle für IT-Governance, dpunkt.verlag, Heidelberg, 2007.

[KÖ06] Kagermann, H.; Österle, H.: Geschäftsmodelle 2010 - Wie CEOs Unternehmen transformieren, Frankfurter Allgemeine Buch, Frankfurt, 2006.

[Kr05] Krcmar, H.: Informationsmanagement, Springer, Berlin, Heidelberg u. a., 2005.

[LHM95] Lehner, F., et al.: Wirtschaftsinformatik, München, Wien, 1995.

[ÖBH92] Österle, H., et al.: Unternehmensführung und Informationssystem: Der Ansatz des St. Gallener Informationssystem-Managements, Teubner, Stuttgart, 1992.

[OGC 2007a] OGC: ITIL V3. Service Strategy, London, 2007.

[OGC 2007b] OGC: ITIL V3. Service Design, London, 2007.

[OGC 2007c] OGC: ITIL V3. Service Transition, London, 2007.

[OGC 2007d] OGC: ITIL V3. Service Operation, London, 2007.

[OGC 2007e] OGC: ITIL V3. Continual Service Improvement (CSI), London, 2007.

[Ös89] Österle, H.: Informationsmanagement in den 90er Jahren, In: Neue Technik, 31, 7, 1989, 27-29.

[RS05] van Reenen, J.; Sadun, R.: Information Technology and Productivity: It ain't what you do it's the way you do I.T., EDS Innovation Research Programme Discussion Paper Series, 2005.

[Sc98] Schwarze, J.: Informationsmanagement, Berlin, 1998.

[Schm96] Schmidt, G.: Informationsmanagement, Springer, Berlin, Heidelberg u. a., 1996.

[TK02] Teubner, A.; Klein, S.: Vergleichende Buchbesprechung - Informationsmanagement, In: Wirtschaftsinformatik, 44, 3, 2002, 285-299.

[TK98] Tallon, P. P.; Kraemer, K. L.: A Process-oriented Assessment of the Alignment of Information Systems and Business Strategy: Implications for IT Business Value, In: Working Paper Graduate School of Management, Irvine, California, 1998.

[VG01] Voß, S.; Gutenschwager, K.: Informationsmanagement, Berlin, 2001.

[ZB03] Zarnekow, R.; Brenner, W.: Konzepte für ein produktorientiertes Informationsmanagement, Konferenzbeitrag, Heidelberg, 2003.

[ZBP06] Zarnekow, R., et al.: Integriertes Informationmanagement, Berlin, 2006.

Betriebserfahrungen mit OTRS

Wilfried Grieger

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Einleitung

Die GWDG hatte sich im Jahr 2004 dazu entschlossen, eingehende Probleme, Anfragen, Aufträge und Fehlermeldungen weitestgehend elektronisch zu verwalten und innerhalb eines Trouble-Ticket-Systems zu bearbeiten. Die Auswahl des Systems wurde bereits ausführlich beschrieben.[1] Die GWDG hatte sich damals für das **O**pen source **T**icket **R**equest **S**ystem (OTRS) entschieden. Die Vorteile dieses Systems waren und sind:

- Open Source Software
- rein HTML-basiert
- Eskalationsmechanismen beliebig programmierbar
- niedrige Anschaffungskosten
- hohe Akzeptanz bei Mitarbeiterinnen und Mitarbeitern der GWDG

1. W. Grieger, Trouble-Ticket-Systeme – Kriterien, Auswahl, Erfahrungen, in: GWDG-Bericht Nr. 67, Göttingen 2005

Die Nachteile des Systems waren und sind:

- keine fertigen Reports
- schlechte Dokumentation

1. Zeitplan von der Auswahl bis zum Produktionsbetrieb

Die folgende Tabelle gibt den Zeitplan wieder, und zwar vom Beginn der Auswahl des Trouble-Ticket-Systems bis zu den letzten Änderungen im Produktionsbetrieb:

	Zeitraum
Auswahl	01/2004 - 09/2004
Installation und Tests	10/2004 - 11/2004
Konfiguration	11/2004 - 01/2005
Schulungen aller Mitarbeiterinnen und Mitarbeiter	01/2005 - 03/2005
Innerbetriebliche Tests	03/2005 - 04/2005
Einsatz für alle Mitarbeiterinnen und Mitarbeiter im Probebetrieb	ab 04/2005
Wartungsvertrag mit der OTRS AG	ab 07/2005
vereinfachte Eingabe von Telefontickets	ab 09/2005
Produktionsbetrieb, Regelungsabrede mit dem Betriebsrat	ab 02/2007
WWW-Customer-Interface	ab 01/2008

Über die Konfiguration des Systems wurde in einer Projektgruppe ausführlich diskutiert und beraten, um bereits zu Beginn eine optimierte sachgerechte Anpassung realisieren zu können. Die Schulung der Mitarbeiterinnen und Mitarbeiter wurde ebenfalls sorgfältig durchgeführt, sodass das System von Anfang an gleich richtig bedient werden konnte.

Da noch sehr viele Anfragen per Telefon eingehen, musste eine vereinfachte Eingabe von Telefontickets geschaffen werden, um auch diese Eingänge

möglichst vollständig zu erfassen. Weiter wurde der Wunsch geäußert, auch Tickets per WWW-Maske eingeben zu können. Dies wurde im Customer-Interface realisiert.

Da ein Trouble-Ticket-System auch Rückschlüsse auf die Arbeit der Mitarbeiterinnen und Mitarbeiter zulässt, musste der Betriebsrat frühzeitig eingebunden werden. Die gemeinsam gefundenen Regeln wurden in der Regelungsabrede niedergeschrieben.

Veröffentlicht wurden die einzelnen erreichten Abschnitte in der Einführungsphase in den GWDG-Nachrichten. In der Ausgabe 4/2005 wurde erstmalig die zentrale E-Mail-Adresse support@gwdg.de bekanntgegeben, ohne jedoch auf das verwendete OTRS hinzuweisen. Dies wurde noch einmal in der Ausgabe 9/2005 wiederholt, um die Akzeptanz der Adresse zu fördern. In der Ausgabe 4/2006 wurde dann OTRS ausführlich vorgestellt, in der Ausgabe 1/2008 mit dem WWW-Customer-Interface.

2. Bearbeitung der Tickets

Die Tickets gehen über die E-Mail-Adresse support@gwdg.de oder über das Customer-Interface zentral ein. Jeder, der ein Ticket einstellt, erhält eine automatische Eingangsbestätigung. Die Mitarbeiterinnen und Mitarbeiter des First Level Supports nehmen jedes Ticket in Empfang.

Wenn das Ticket im First Level Support bearbeitet werden kann, wird es auch dort bearbeitet und möglichst erfolgreich geschlossen.

Wenn das Ticket im First Level Support nicht bearbeitet werden kann, wird es von einer Mitarbeiterin oder einem Mitarbeiter im First Level Support in eine themenbezogene Queue oder Unterqueue des OTRS verschoben. Diese Queues und damit auch die dorthin verschobenen Tickets sind für die Mitarbeiterinnen und Mitarbeiter des Second Level Supports zugänglich und werden von ihnen dort bearbeitet.

Damit Tickets nicht unbearbeitet liegenbleiben, sind mindestens zwei Mitarbeiterinnen und Mitarbeiter für die Bearbeitung in einer Queue eingeteilt. Damit werden Fehlzeiten weitestgehend ausgeglichen.

Wenn die Tickets trotzdem nicht bearbeitet werden sollten, sorgt ein Eskalationsmechanismus dafür, dass die Vorgesetzten der für die Queue zuständigen Mitarbeiterinnen und Mitarbeiter informiert werden. Die Vorgesetzten wiederum ergreifen dann weitere Maßnahmen, damit das Ticket erfolgreich geschlossen werden kann.

3. Im OTRS eingerichtete Queues

Die folgenden Queues (Oberqueues) sind im OTRS der GWDG eingerichtet:

- Anwendungen und Informationssysteme
- Benutzerverwaltung und Accounting
- Betriebssysteme und Basissoftware
- E-Mail
- Kurse
- Netzwerk
- Rechnerhardware und Peripherie
- Sicherheit
- Sonstiges
- WWW

Unter diesen Oberqueues befinden sich in einer zusätzlichen Ebene noch Unterqueues zur weiteren Unterteilung der Thematiken. Insgesamt handelt es sich dabei um ca. 60 Queues. Die Namen der Queues sind so gewählt, dass sie die dort behandelten Thematiken erkennen lassen.

4. Bisher bearbeitete Tickets

Im Zeitraum vom 01.02.2007 bis zum 31.10.2008 wurden insgesamt 4.725 Tickets bearbeitet. Dabei wurden bereits 2.225 Tickets (47 %) vom First Level Support erfolgreich geschlossen. 2.500 Tickets (53 %) mussten an den Second Level Support weitergereicht werden.

Im Second Level Support teilen sich die Tickets folgendermaßen auf die Queues auf:

Queue	Tickets
Anwendungen und Informationssysteme	4 %
Benutzerverwaltung und Accounting	8 %
Betriebssysteme und Basissoftware	29 %
E-Mail	27 %

Queue	Tickets
Kurse	1 %
Netzwerk	17 %
Rechnerhardware und Peripherie	4 %
Sicherheit	2 %
Sonstiges	5 %
WWW	4 %

Wider Erwarten scheint es bei der Sicherheit von IT-Systemen nur wenig Probleme zu geben.

5. Vorteile bei der Nutzung von OTRS

Zur Zusammenfassung sollen hier noch einmal die Vorteile dargestellt werden, wenn das OTRS genutzt wird:

- garantierte Erreichbarkeit mindestens einer Mitarbeiterin oder eines Mitarbeiters
- Tickets werden nicht „vergessen“!
- Eskalation von verzögert bearbeiteten Tickets
- lückenlose Aufzeichnung der Maßnahmen, Nachverfolgung
- Kunden- und Bearbeiter-Schnittstelle per WWW-Browser und per E-Mail
- Ziel: Erstellung einer Wissensbasis

6. Für OTRS Zuständige bei der GWDG

Für die OTRS-Server-Administration ist Herr Michael Binder, mbinder@gwdg.de, zuständig. Die OTRS-Administration hat Herr Dr. Thomas Otto, totto@gwdg.de, übernommen, der von Frau Sigrun Greber, sgreber @gwdg.de, vertreten wird.

In der Reihe GWDG-Berichte sind zuletzt erschienen:

Nähere Informationen finden Sie im Internet unter
`http://www.gwdg.de/gwdg-berichte`

Nr. 40 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1994
1995

Nr. 41 *Brinkmeier, Fritz* (Hrsg.):
Rechner, Netze, Spezialisten. Vom Maschinenzentrum zum Kompetenzzentrum - Vorträge des Kolloquiums zum 25jährigen Bestehen der GWDG
1996

Nr. 42 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1995
1996

Nr. 43 *Wall, Dieter* (Hrsg.):
Kostenrechnung im wissenschaftlichen Rechenzentrum - Das Göttinger Modell
1996

Nr. 44 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1996
1997

Nr. 45 *Koke, Hartmut und Engelbert Ziegler* (Hrsg.):
13. DV-Treffen der Max-Planck-Institute - 21.-22. November 1996 in Göttingen
1997

Nr. 46 **Jahresberichte 1994 bis 1996**
1997

Nr. 47 *Heuer, Konrad, Eberhard Mönkeberg und Ulrich Schwardmann*:
Server-Betrieb mit Standard-PC-Hardware unter freien UNIX-Betriebssystemen
1998

Nr. 48 *Haan, Oswald* (Hrsg.):
Göttinger Informatik Kolloquium - Vorträge aus den Jahren 1996/97
1998

Nr. 49 *Koke, Hartmut und Engelbert Ziegler* (Hrsg.):
IT-Infrastruktur im wissenschaftlichen Umfeld - 14. DV-Treffen der Max-Planck-Institute, 20. - 21. November 1997 in Göttingen
1998

Nr. 50 *Gerling, Rainer W.* (Hrsg.):
Datenschutz und neue Medien - Datenschutzschulung am 25./26. Mai 1998
1998

Nr. 51 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1997
1998

Nr. 52 *Heinzel, Stefan und Theo Plesser* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1998
1999

Nr. 53 *Kaspar, Friedbert und Hans-Ulrich Zimmermann* (Hrsg.):
Internet- und Intranet-Technologien in der wissenschaftlichen Datenverarbeitung - 15. DV-Treffen der Max-Planck-Institute, 18. - 20. November 1998 in Göttingen
1999

Nr. 54 *Plesser, Theo und Helmut Hayd* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1999
2000

Nr. 55 *Kaspar, Friedbert und Hans-Ulrich Zimmermann* (Hrsg.):
Neue Technologien zur Nutzung von Netzdiensten - 16. DV-Treffen der Max-Planck-Institute, 17. - 19. November 1999 in Göttingen
2000

Nr. 56 *Plesser, Theo und Helmut Hayd* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2000
2001

Nr. 57 *Hayd, Helmut und Rainer Kleinrensing* (Hrsg.):
17. und 18. DV-Treffen der Max-Planck-Institute
22. - 24. November 2000 in Göttingen
21. - 23. November 2001 in Göttingen
2002

Nr. 58 *Plesser, Theo und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2001
2003

Nr. 59 *Suchodoletz, Dirk von*:
Effizienter Betrieb großer Rechnerpools - Implementierung am Beispiel des Studierendennetzes an der Universität Göttingen
2003

Nr. 60 *Haan, Oswald* (Hrsg.):
Erfahrungen mit den IBM-Parallelrechnersystemen RS/6000 SP und pSeries690
2003

Nr. 61 *Rieger, Sebastian:*
Streaming-Media und Multicasting in drahtlosen Netzwerken - Untersuchung von Realisierungs- und Anwendungsmöglichkeiten
2003

Nr. 62 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2002
2003

Nr. 63 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2003
2004

Nr. 64 *Koke, Hartmut* (Hrsg.):
GÖ* – Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Vorantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“
2004

Nr. 65 *Koke, Hartmut* (Hrsg.):
GÖ* – Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Hauptantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“
2004

Nr. 66 *Bussmann, Dietmar und Andreas Oberreuter* (Hrsg.):
19. und 20. DV-Treffen der Max-Planck-Institute
20. - 22. November 2002 in Göttingen
19. - 21. November 2003 in Göttingen
2004

Nr. 67 *Gartmann, Christoph und Jochen Jähnke* (Hrsg.):
21. DV-Treffen der Max-Planck-Institute
17. - 19. November 2004 in Göttingen
2005

Nr. 68 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2004
2005

Nr. 69 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2005
2006

Nr. 70 *Gartmann, Christoph und Jochen Jähnke* (Hrsg.):
22. DV-Treffen der Max-Planck-Institute
16. - 18. November 2005 in Göttingen
2006

Nr. 71 *Hermann, Klaus und Jörg Kantel* (Hrsg.):
23. DV-Treffen der Max-Planck-Institute
15. - 17. November 2006 in Berlin
2007

Nr. 72 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2006
2007

Nr. 73 *Baumann, Thomas, Dieter Ruder und Bertram Smolny* (Hrsg.):
24. DV-Treffen der Max-Planck-Institute
6. - 8. November 2007 in Jena
2008

Nr. 74 *Schwardmann, Ulrich* (Hrsg.):
Grid-Technologie in Göttingen - Beiträge zum Grid-Ressourcen-Zentrum GoeGrid
2009

Nr. 75 *Baumann, Thomas, Dieter Ruder und Bertram Smolny* (Hrsg.):
25. DV-Treffen der Max-Planck-Institute
18. - 20. November 2008 in Göttingen
2009