eckhard HAUENHERM

Effiziente Kommunikation im Unternehmen

Konzepte & Lösungen mit Microsoft-Plattformen

Skype for Business 2015

SharePoint 2016

MS Office 2016

Exchange 2016

Active Directory

Windows Server 2016

HANSER

Im Internet:
Praxisbeispiele mit Office 365

Hauenherm

Effiziente Kommunikation im Unternehmen:
Konzepte & Lösungen mit Microsoft-Plattformen

Eckhard Hauenherm

Effiziente Kommunikation im Unternehmen: Konzepte & Lösungen mit Microsoft-Plattformen

SharePoint 2016, Exchange 2016,
MS Office 2016, Skype for Business 2015,
Active Directory, Windows Server 2016

HANSER

Der Autor:
Eckhard Hauenherm, Essen
www.hauenherm.de

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Sylvia Hasselbach
Copy editing: Walter Saumweber, Ratingen
Umschlagdesign: Marc Müller-Bremer, München, www.rebranding.de
Umschlagrealisation: Stephan Rönigk
Gesamtherstellung: Kösel, Krugzell
Printed in Germany

Print-ISBN: 978-3-446-44681-6
E-Book-ISBN: 978-3-446-44911-4

Inhalt

Vorwort

Dieses Buch erzählt eine Geschichte. Das mag ein wenig erstaunen für ein IT-Buch. Die Geschichte, die mein Buch erzählt, ist der Versuch, das umzusetzen, was Bill Gates im Jahr 2000 in seinem Buch „Digitales Business“ beschrieben hat, nämlich die Abbildung herkömmlicher Geschäftsprozesse mit Mitteln der Informationstechnologie. Dabei beschränke ich mich auf das, was ich Kommunikationsprozesse nenne, also Prozesse, die auf klassischen Kommunikationsverfahren wie Informationsverteilung, Antragstellung und Genehmigung, Auskunftserteilung und Ähnlichem basieren.

Natürlich versuchen wir das hier mit der IT-Infrastruktur, die Microsoft, das von Bill Gates gegründete Unternehmen, uns bietet. Wir werden also Produkte einsetzen wie Windows Server und Clients, die Microsoft Office-Anwendungen, SharePoint Server, Exchange Server, Skype for Business und dabei auch Windows-Dienste nutzen wie die Zertifikatsdienste, die Federation Services und die Rechteverwaltungsdienste (Active Directory Rights Management Services). Die Anforderungen lassen sich natürlich auch in anderen Plattformen umsetzen, wie zum Beispiel in einer Lotus Notes/Domino-Infrastruktur. Es würde aber den Rahmen eines solchen Buches sprengen, beides zu beschreiben. Außerdem geht dabei ein großer Teil der Praxisorientierung des Buches verloren. Und letzten Endes glaube ich, dass die Microsoft-Umgebung mit den aktuellen Anwendungen tatsächlich die Anforderungen am vollständigsten abdecken kann (wobei natürlich auch im Blick zu behalten ist, dass wir dazu eine ganze Reihe von Produkten von Microsoft einsetzen müssen).

Die Beschreibung folgt, nach einigen theoretischen Einführungen, dem Ablauf eines solchen Projektes in einem mittelständischen Unternehmen. Dazu beschreibe ich ein Musterunternehmen, für das ich meines Erachtens typische Anforderungen ermittle, wie ich sie im Rahmen meiner eigenen Projekte immer wieder zu lösen gehabt habe. Auch wenn diese Anforderungen natürlich nicht auf jedes Unternehmen übertragbar sind, so gehe ich doch davon aus, dass sich in der Summe der Beispiele viele Umsetzungsszenarien wiederfinden, die sich auch in anderen, womöglich auch im Unternehmen des Lesers anwenden lassen.

Eine zweite Einschränkung habe ich mir dabei noch auferlegt. In der Umsetzung nutze ich nur die Werkzeuge und Funktionen, die mit den eingesetzten Anwendungen zur Verfügung stehen. Ich verzichte also vollständig auf Werkzeuge von sogenannten Drittanbietern. In meinen Projekten bin ich immer wieder darüber erstaunt, wie weit sich auch sehr spezielle Anforderungen schon mit den Bordmitteln der oben genannten Infrastrukturkomponenten umsetzen lassen.

Die Idee für dieses Buch hatte ich, als Microsoft die Produktversionen des Jahres 2010 der genannten Produkte auf den Markt brachte. Diese Versionen boten meines Erachtens zum ersten Mal die Möglichkeit, die in Frage stehenden Anforderungen durchgängig mit einer sinnvollen und effizienten Kombination dieser Produkte umzusetzen. Dies konnte ich auch in vielen Projekten realisieren, häufig sogar zur Überraschung der Auftraggeber.

In der Beschreibung nutzen wir natürlich die aktuelle Produktpalette des Jahres 2016, also Windows 10, Windows Server 2016, Exchange 2016, SharePoint 2016 und Skype for Business 2015. Viele der hier beschriebenen Szenarien lassen sich aber auch mit älteren Versionen der Plattformen, insbesondere derjenigen aus dem Jahr 2013 umsetzen. Im Detail sind dabei eventuell leicht abweichende Einstellungen vorzunehmen. Wenn diese nicht offensichtlich sind, werde ich versuchen, die Unterschiede mit zu beschreiben. Selbst wenn Sie noch die 2010er-Versionen einsetzen, werden Sie viele Tipps finden, die auch damit funktionieren. Soweit werde ich aber in der Beschreibung nicht zurückgehen. Die dazu erforderlichen Einstellungen zu finden, überlasse ich dem Leser.

Was können Sie nun von diesem Buch erwarten? Es ist kein Buch über die Installation von Servern oder den Aufbau einer solchen Infrastruktur. In der Beschreibung gehe ich davon aus, dass die einzelnen Komponenten nach den Best Practices installiert sind. In meinen Fall habe ich die notwendige Umgebung der Einfachheit halber in Microsoft Cloud Service Azure aufgebaut, in der ich dann die Umsetzung teste und die erläuternden Screenshots erstelle.

Auch auf die erforderlichen Einstellungen der Grundkonfiguration der Anwendungen werde ich nur insoweit eingehen, als sie für die spezifische Umsetzung erforderlich beziehungsweise spezifisch sind.

Was aber dieses Buch bietet, ist die konkrete Beschreibung, wie die genannten Prozesse umgesetzt werden können und welche Einstellungen dabei vorzunehmen sind. In Teilen wird das durchaus in Form von „Klickanleitungen“ passieren, insbesondere bei den ersten Schritten der Umsetzung. In den meisten Fällen gehe ich aber davon aus, dass die Leser dieses Buches nach den ersten Schritten über genügend Erfahrung mit den Anwendungen verfügen, um die weiteren Schritte selbständig vorzunehmen, wenn die notwendigen Einstellungen benannt sind.

Auch wenn die Zielgruppe somit in erster Linie sogenannte Power-User und Administratoren der Anwendungen sind, also Anwender, die sich auch die Umsetzung spezifischer Anforderungen zutrauen, so werden doch auch andere Rollen des Unternehmens eingebunden. In der Beschreibung habe ich dazu auch das Personal meines Musterunternehmens genutzt und die Geschichte so beschrieben, dass die notwendigen Schritte jeweils von dem entsprechenden Rolleninhaber vorgenommen werden. Dies soll unter anderem auch deutlich machen, auf welcher Berechtigungsebene Einstellungen vorgenommen werden müssen, und wie diese in einem Unternehmen zu entscheiden sind. Meines Erachtens erlangen die Beschreibungen dadurch eine höhere Realitätsnähe, als wenn alles immer nur von einem „gottgleichen“ Unternehmensadministrator durchgeführt wird. Außerdem wird auch nur so deutlich, wie die Prozesse, mit denen ja in erster Linie die „normalen“ Anwender arbeiten müssen, gestaltet werden können und müssen, damit sie effizient genutzt werden können.

An einigen Stellen stößt man dabei natürlich auch auf Probleme oder stellt fest, dass die konkrete Umsetzung deutlich komplexer ist, als zuerst gedacht. Dies ist das Gebiet, in dem

sich dann Zusatzprodukte einbringen können. Der Markt dafür ist inzwischen recht groß und teilweise auch unübersichtlich geworden. Auch wenn ich selbst in meinen Projekten hin und wieder auf Zusatzprodukte zurückgreife, so werde ich in diesem Buch dennoch an meiner Leitlinie festhalten und beschreiben, was mit den vorhandenen Mitteln umsetzbar ist. Im Gegensatz zu den typischen Herstelleranleitungen werde ich die Einschränkungen mit ihren Auswirkungen jedoch benennen.

Dieses Buch hat zwar nur einen Autor, ein solches Vorhaben ist in der Praxis aber kaum im Alleingang zu stemmen. Ich hatte den großen Vorteil, dass ich eine Reihe von Kollegen mit Fragen »löchern« und mit Ihnen meine Ideen austauschen konnte.

Außerdem danke ich Sylvia Hasselbach, die das Buch betreut hat, und Sieglinde Schärl vom Hanser Verlag sowie meinem Korrektor Walter Saumweber. Ohne sie wäre dieses Buch nicht zustande gekommen. Meiner Familie danke ich für die Geduld während meiner Arbeit an dem Buch.

Schließlich geht noch ein großer Dank an meine Kunden. Ohne sie hätten die hier dargestellten Ideen nicht entstehen und wachsen können.

Eckhard Hauenherm,

Essen im August 2017

1 Warum dieses Buch, was es bietet (und was nicht)

Im Jahr 1999 veröffentlichte Bill Gates ein Buch mit dem Titel „Digital Business“. Darin beschreibt er die damals erkennbaren Möglichkeiten der Unterstützung von Unternehmensprozessen mit IT und entwirft einen Ausblick auf die fortschreitende Digitalisierung im Unternehmen. Seit damals hat sich die IT enorm weiterentwickelt. Wenn man die Entwicklung bei Microsoft verfolgt hat, war unübersehbar, wie die Idee der durchgängigen Prozessunterstützung im Unternehmen umgesetzt werden konnte. Insbesondere die immer weitere fortschreitende Integration der verschiedenen Werkzeuge lieferte neue Möglichkeiten, Prozesse vom Anwender bis zur unternehmensweiten Datenauswertung mit abzubilden.

Diese Integration wird einerseits an einzelnen Produkten wie SharePoint deutlich, andererseits auch an der immer stärkeren Vernetzung einzelner Anwendungen.

Die erste Version von SharePoint, im Jahr 2000 unter dem internen Namen *Tahoe Server* von Microsoft entwickelt, bot im Schwerpunkt Funktionen zur Verwaltung von Dokumenten. Nach und nach sind in dieses Produkt verschiedene Spezialanwendungen integriert worden, von Content Management-Funktionen (Content Management Server) bis hin zur Business Intelligence (Performance Point Server), nicht zu vergessen spezifische Anwendungen wie Project Server. Mit der Version 2010 hatte Microsoft diesen Prozess weitgehend abgeschlossen. Die nachfolgenden Versionsentwicklungen dienten der Verbesserung der Funktionen. In den aktuellen Versionen 2013 und 2016 wird der Prozess zum Teil wieder umgekehrt und einige Funktionen werden aus SharePoint in eigene Serverprodukte ausgelagert, wie z. B. die Office Web Apps, die Workflow-Komponente oder einige der Business Intelligence-Funktionen.

Ein weiterer wichtiger Schritt für die Integration war die Entwicklung des Active Directorys in Windows 2000, ebenfalls in der ersten Version um die Jahrtausendwende vorgestellt. Wenn man heutzutage Microsoft-Umgebungen in Unternehmen aufsetzt, wird einem sehr schnell bewusst, wie viele Anwendungen auf die Grundstrukturen dieses Verzeichnisdienstes aufsetzen und wie weit darüber die Integration sichergestellt wird. Das fängt an mit den Prozessen der Namensauflösung, der Berechtigungssteuerung bis zur Dienstkontenverwaltung und Konfigurationssicherung (z. B. in Exchange 2010/2013).

Die Idee für dieses Buch ist aus der täglichen Arbeit mit diesen Abhängigkeiten in meinen Beratungsprojekten entstanden. Viele dieser Projekte starteten als Implementierungen einzelner Anwendungen (z. B. SharePoint oder Exchange) und endeten als Integrations- und Änderungsprojekte, die viele Bereiche im Unternehmen und in der IT einbinden. Viele

Unternehmen scheitern dabei daran, das Integrationspotential zu heben und bleiben bei einem Parallelbetrieb einzelner Anwendungen stehen. Damit gehen aber auch wirtschaftliche und organisatorische Vorteile verloren.

Ziel dieses Buches ist es, die nächsten Schritte aufzuzeichnen, die ein Unternehmen gehen kann, um zu einer wirklich integrierten Umsetzung seiner Prozesse zu kommen.

IT-Prozesse dienen primär der Verarbeitung und Übermittlung von Information. In der Wissenschaft wird die Weitergabe und Verarbeitung von Information allgemein als Kommunikation beschrieben. Somit gehe ich in diesem Buch davon aus, dass die zu betrachtenden Anforderungen die Kommunikationsanforderungen in Unternehmen sind. Unternehmenskommunikation lässt sich auf dieser Betrachtungsebene immer als Prozess beschreiben. Wie der Beschreibungsansatz aussehen kann, werde ich im zweiten Kapitel dieses Buches verdeutlichen. Das Beschreibungsmodell ist unabhängig von den einzusetzenden Produkten. Auch wenn dieses Buch die Umsetzung anhand der Microsoft-Plattformen beschreibt, ist die Umsetzung natürlich auch mit anderen Produkten grundsätzlich möglich. Die Microsoft-Plattform habe ich für dieses Buch aus zwei Gründen gewählt. Erstens hat Microsoft, wie oben schon angedeutet, in seiner Produktpalette meiner Ansicht nach den höchsten Integrationsgrad erreicht und bietet dabei für alle Anforderungen die passenden Werkzeuge an und zweitens sind mir diese Werkzeuge aus meinen eigenen Projekten am vertrautesten.

Neben den oben schon angesprochenen Produkten werden für eine vollständige Umsetzung der Kommunikationsanforderungen weitere Anwendungen genutzt. Auf der Ebene des Active Directorys sind das insbesondere die Zertifikatsdienste, das Management digitaler Rechte und die Verbunddienste. Für die Datenhaltung ist in einer Microsoft-geprägten Umgebung SQL Server zuständig, der wiederum von vielen anderen Anwendungen genutzt wird. Natürlich werden klassische Kommunikationswerkzeuge wie Exchange und SharePoint genutzt, aber auch neuere Produkte wie Lync (jetzt Skype for Business) werden zur Realisierung spezifischer Anforderungen der Echtzeitkommunikation eingebunden. Da die Kommunikation immer am Ende den Desktop des Anwenders als Ein-und Ausgabewerkzeug nutzt, sind natürlich auch die Office-Anwendungen selbst mit zu betrachten.

Da sich dieses Buch auf den „zweiten“ Schritt – den Schritt der Integration –, konzentriert, wird hier nicht der Aufbau der Systemumgebung beschrieben, sondern davon ausgegangen, dass die Server im Unternehmen schon installiert und konfiguriert sind. Die Serverkonfiguration wird allerdings dann angesprochen, wenn sie für die Zurverfügungstellung spezifischer Funktionen beachtet werden muss.

Viele Unternehmen beschäftigen sich derzeit mit Cloud-Strategien. Bei den in diesem Buch beschriebenen Szenarien stellt sich natürlich sofort die Frage, ob diese Ansätze auch in der Cloud umsetzbar sind. Microsoft bietet inzwischen mit Office 365 eine leistungsfähige Cloudlösung, die genau die hier angesprochenen Produkte nutzt. Daher wird im letzten Kapitel der Frage nachgegangen, inwieweit die hier präsentierten Lösungen auch mit Office 365 umsetzbar sind.

Da es sich bei diesem Buch um einen administrativen Leitfaden handeln soll, habe ich einen Ansatz gewählt, der die Umsetzung von den Anforderungen her beschreibt. Konkret werde ich ein Musterunternehmen mit typischen Funktionsbereichen beschreiben und ausgehend von den spezifischen Aufgaben und Anforderungen der einzelnen Abteilungen die Umsetzung der Prozesse beschreiben.

2 Das Unternehmen als kommunikatives System

Kommunikation ist eine Form menschlichen Handelns. Das heißt, dass wir mit Kommunikation Ziele erreichen wollen. In der Linguistik spricht man von der Illokution einer sprachlichen Handlung oder auch kurz von illokutionären Akten (die Linguisten verzeihen mir bitte diese etwas vereinfachte Darstellung, für unsere Zwecke ist sie hier jedoch ausreichend). Meines Erachtens liefert uns diese Sichtweise über Kommunikation einen der wichtigsten Aspekte für die Planung und Gestaltung von Kommunikationsverfahren, nämlich den Faktor des Erfolges. Erfolg ist, einfach gesprochen, nichts anderes als das Erreichen von Zielen. Wenn wir also wissen, welches Ziel oder Ergebnis mit einem kommunikativen Akt erreicht werden soll, haben wir eine Möglichkeit, den Erfolg der Kommunikation zu messen.

Auch wenn es einige Arten sprachlichen Handelns geben mag, die nicht direkt auf eine Reaktion unseres Gesprächspartners abzielen (z. B. Flüche), so zielen doch die meisten unserer Äußerungen darauf ab, etwas bei unserem Gegenüber zu erreichen und eine Handlung auszulösen. Auf eine Frage möchten wir eine Antwort, mit einer Bitte Unterstützung bekommen. Mit einer Entschuldigung möchten wir erreichen, dass der Andere uns vergibt. Dabei spielt es keine Rolle, ob es sich um eine einfache Äußerung handelt oder um einen komplexen Text. Auch ein Geschäftsbericht dient dazu, beim Empfänger einen Erkenntnisgewinn zu erreichen. Komplexe Äußerungen verfolgen häufig nicht nur ein, sondern mehrere Ziele. So wird in Geschäftsberichten neben der reinen Information häufig auch versucht, eine positive Wahrnehmung beim Empfänger zu erreichen.

2.1 Wie kommunizieren Unternehmen?

Mit diesem letzten Beispiel sind wir bereits bei der Unternehmenskommunikation angelangt. Unternehmen kommunizieren und in Unternehmen wird kommuniziert. Um es genauer zu sagen, der größte Teil administrativer Aufgaben im Unternehmen besteht aus kommunikativen Handlungen. Auch Unternehmensmanagement besteht zu ca. 90 % aus Kommunikation. Sie erkennen schon, mir geht es weniger um Unternehmenskommunikation im Sinne von Marketing und Public Relations, also um die Kommunikation des Unternehmens an sich (die Arten von Kommunikation, in denen das Unternehmen und nicht die

darin arbeitenden Personen als »Sprecher« auftritt), sondern um die Kommunikation innerhalb des Unternehmens, z. B. die Informationsflüsse zwischen Abteilungen oder die Kontakte zu externen Gesprächspartnern wie Ansprechpartnern anderer Unternehmen. Sicherlich spielen dabei auch Aspekte der Außendarstellung des Unternehmens eine Rolle. Ich möchte aber kein Buch über Marketing oder Public Relations schreiben. Daher wird der Aspekt der Außendarstellung in diesem Buch nur als eine mögliche Anforderung unter anderen an die Kommunikation mit externen Geschäftspartnern eine Rolle spielen. Im weiteren Verlauf werde ich zeigen, wie diese Kommunikationsprozesse durch moderne IT-Werkzeuge (am Beispiel der Microsoft-Plattformen) optimal unterstützt werden. Nachfolgend finden Sie eine – naturgemäß unvollständige – Liste typischer kommunikativer Akte in Unternehmen:

- Bestellungen auslösen
- Angebote einholen
- Stellen ausschreiben
- Verhandlungen führen
- Material anfordern
- Termine vereinbaren
- Dienstreisen buchen
- Spesen abrechnen
- Monatszahlen berichten
- Mitarbeiter anweisen
- Personal beurteilen
- Ziele vereinbaren

Für die meisten dieser Handlungen nutzen wir heute IT-Werkzeuge. Angebote schreiben wir in einer Textverarbeitung und versenden sie per E-Mail. Für Terminvereinbarungen nutzen wir elektronische Kalender, Stellen werden in Online-Portalen und -Medien ausgeschrieben, kaufmännische Zahlen aus verschiedenen Datenquellen zusammengetragen, in einer Tabellenkalkulation ausgewertet und als digitales Dokument versendet oder veröffentlicht.

Allerdings enthält diese Liste auch einige Kommunikationsarten, die wir nicht oder nur teilweise durch IT unterstützen. So führen wir z. B. Mitarbeitergespräche in der Regel nicht über E-Mail oder Telefon, sondern bevorzugen immer noch das persönliche Gespräch. Nicht alle Kommunikationsmedien sind für das Erreichen bestimmter kommunikativer Ziele gleichermaßen geeignet. Genau darum geht es in diesem Buch. Ich möchte nicht nur zeigen, wie sich kommunikative Anforderungen mit aktuellen Werkzeugen umsetzen lassen, sondern auch, welche Werkzeuge sich für welche Arten kommunikativer Handlungen im Unternehmen eignen und natürlich auch, welche Kriterien für die Entscheidung eine Rolle spielen.

Viele der oben genannten Handlungen sind im Unternehmen aufeinander bezogen bzw. setzen einander voraus. Bestellungen basieren auf Angeboten, Zielvereinbarungsgespräche setzen Terminvereinbarungen voraus etc. Wenn man diese Abhängigkeiten über alle kommunikativen Handlungen im Unternehmen analysiert, sieht man relativ schnell, dass sich ein Unternehmen als ein System kommunikativer Handlungen, oder kurz als kommunika-

tives System, beschreiben lässt. Im Grunde genommen bekommt man mit einer vollständigen Beschreibung eine Landkarte der Kommunikation im Unternehmen, wie man sie in der Prozessanalyse als Prozesslandschaft des Unternehmens mit Kernprozessen und Unterstützungsprozessen kennt.

2.1.1 Kommunikationswege im Unternehmen

Wenn wir uns in einer Landschaft zurechtfinden wollen, nutzen wir dafür in der Regel eine Landkarte. Das Bild der Landkarte eignet sich hervorragend als Metapher für die Beschreibung der unterschiedlichen Arten der Unternehmenskommunikation. Eine Landkarte oder besser ein Stadtplan zeigt uns, über welche Wege wir von einem Ort zum anderen gelangen können. In der Regel werden dabei Straßen, verschiedene Verkehrsmittel (Eisenbahn, Fähren) und Knotenpunkte als Übergabepunkte (Kreuzungen, Häfen, Flughäfen, Bahnhöfe) dargestellt. Stellen wir uns eine Organisation bzw. ein Unternehmen im Folgenden einfach als eine Stadt vor. Der Stadtplan weist den (kommunikativen) Weg durch diese Stadt und wir versuchen herauszufinden, welche Wege die kürzesten bzw. effizientesten sind.

Einige Informationsflüsse (auch dies sind kommunikative Akte) sind in Unternehmen strikt vorgegeben und erlauben keine Abweichungen. Die Kommunikationspartner können nicht selbständig über den Ablauf der Kommunikation entscheiden, sondern müssen sich an einen vorgegebenen Prozess halten. Dies ist häufig bei klassischen Antrags- oder Bestellprozessen der Fall, insbesondere wenn das Ergebnis eine Standardaktion darstellt, wie etwa die Bereitstellung neuen Druckerpapiers. In unserem Stadtplan entsprächen diese Prozesse schienengebundenen Transporten. Es gibt einen dedizierten Punkt, an dem die benötigten Informationen eingegeben werden (der Bahnhof, an dem Sie einsteigen können) und der Prozess (also der Zug) bringt Sie bzw. Ihre Informationen über einen vorgegebenen Weg ans Ziel. Diese Prozesse zeichnen sich dadurch aus, dass sie hochgradig automatisierbar sind. Nichtsdestotrotz sind auch sie genau zu planen, schließlich müssen ja genau die Informationen übermittelt werden, die dazu führen, dass am Ende das Druckerpapier an den Arbeitsplatz geliefert wird (Sie erinnern sich: Kommunikation ist Handlung, will also Ziele erreichen).

Wenn in einem solchen Prozess verschiedene Kommunikationssysteme, wie z. B. Telefon, E-Mail oder auch Briefe, angesprochen werden, erweitern wir unsere Stadtplanmetapher einfach um weitere Transportmöglichkeiten, wie z. B. Schiffe. In den Häfen werden die Informationen vom Zug auf ein Schiff verladen. Eventuell werden dabei kleinere Einheiten auch zu größeren zusammengefasst. In unserem Beispiel könnte das heißen, dass die einzelnen Bestellungen zu einer Großbestellung beim Lieferanten zusammengefasst werden, um Kostenvorteile zu nutzen. Ähnlich lassen sich viele kaufmännische Controllingprozesse beschreiben. Auch hier werden strikt vorgegebene Zahlen einzelner Abteilungen zu umfassenden Auswertungen zusammengefasst und weiter berichtet.

Andere Kommunikationsarten im Unternehmen erlauben den Kommunikationspartnern mehr Variationsmöglichkeiten. Dies sind z. B. Verhandlungen oder Gespräche, wie Zielvereinbarungsgespräche. Hier haben wir ein Ziel, das am Ende erreicht werden soll, können aber den Weg dahin, zumindest in gewissem Rahmen, selbst definieren. Auf unserem Stadtplan entsprechen diese Kommunikationsarten dem Individualverkehr auf der Straße. Wir

starten mit unserem Verkehrsmittel, z. B. einem Fahrrad, und haben in der Regel einen Plan des Weges, den wir nehmen wollen. Sobald wir aber auf dem geplanten Weg nicht weiterkommen, wählen wir einen anderen. Im Straßenverkehr treffen wir diese Entscheidungen an Kreuzungen oder Abzweigungen. Übertragen wir das Bild auf unsere Kommunikation, dann entsprechen diese Kreuzungen also den Entscheidungspunkten in Gesprächen oder den Auswahlmöglichkeiten in Prozessen. Wie im Straßenverkehr sind wir dabei in unserer Kommunikation teilweise an Anweisungen und Richtlinien gebunden, die uns im Verkehr als Straßenschilder oder Verkehrsregeln begegnen. Beispielsweise dürfen wir nicht von der falschen Seite in eine Einbahnstraße einfahren. In der Kommunikation finden wir diese Einschränkungen ebenfalls als Richtlinien, z. B. für die Vertraulichkeit der Kommunikation oder für die Aufbewahrung von Dokumenten, wieder.

Aber nicht nur Kreuzungen sind Knotenpunkte in einem Stadtplan. Städte verfügen häufig auch über Stellen, an denen viele Straßen zusammenlaufen und der Verkehr zusammengefasst und eventuell neu verteilt wird, wie z. B. auf Plätzen. Auch dazu finden wir ein Pendant in der Unternehmenskommunikation, nämlich die Kommunikationsverfahren, die Informationen zusammenfassen. Häufig finden wir solche Verfahren in aggregierenden und verteilenden Prozessen, die Informationen über die Hierarchieebenen im Unternehmen hinweg vermitteln. Berichten z. B. Vertriebsmitarbeiter regelmäßig über ihren Umsatz und werden diese Zahlen nach Gebieten und Produkten zusammengefasst, so dass daraus wieder ein umfassender Bericht für die Geschäftsführung entsteht, liegt solch ein aggregierender Prozess vor.

Kommunikationsverfahren dieser Art sind naturgemäß schwieriger zu planen und zu steuern. Insbesondere ist hier zu entscheiden, bis zu welchem Grad strikte Vorgaben sinnvoll sind oder eher die Produktivität einschränken. Einerseits müssen die Zahlen zusammengefasst werden, andererseits sollen auch besondere Ereignisse oder Abweichungen benannt und erläutert werden können.

Selbst für vollständig ungesteuerte Kommunikationsarten finden wir ein Gegenstück in unserer Metapher. Die typischen Abkürzungen und Trampelpfade, die wir insbesondere dann nutzen, wenn wir zu Fuß unterwegs sind. Diese entsprechen geduldeten Kommunikationswegen, die es in jedem Unternehmen gibt, die aber nicht vorgegeben oder gar geplant sind, in vielen Fällen trotzdem sehr effizient eingesetzt werden. Grundsätzlich ist es auch im Unternehmen sinnvoll, die Möglichkeit solch unstrukturierter Kommunikation vorzusehen, da darüber sehr häufig wichtige Informationen verteilt werden. Dies kennt man aus den Analysen des Wissensmanagements. Wissen verbreitet sich in Unternehmen sehr häufig eben nicht über strukturierte Verfahren, sondern immer noch sehr viel stärker über den informellen Austausch in den sogenannten »Teeküchengesprächen«. Allerdings verbreiten sich darüber auch Meinungen und Vorurteile sehr schnell, die nicht auf fundiertem Wissen basieren.

Analog zu den Wegen in einer Stadt lassen sich im Unternehmen also die folgenden Kommunikationswege definieren:

- Große Straßen und Schienenstränge, die Stadteile miteinander verbinden. Diesen entsprechen unsere häufig stark formalisierten Kommunikationswege, über die das Unternehmen Standardaufgaben abwickelt und Informationen sammelt und verteilt. In einer Stadt enden solche Wege häufig an großen Plätzen (z. B. an einem Bahnhofsvorplatz). Hier wird der Verkehr verteilt bzw. gesammelt. Entsprechend werden Informationen in der

Kommunikation im Laufe solcher Prozesse zusammengefasst und über aggregierende Kommunikationsprozesse weitergeleitet oder verteilt.

- Kleinere Straßen. Diese stellen das Sinnbild für weniger formalisierte Kommunikationswege dar, bei denen wir individuelle Entscheidungen für den weiteren Kommunikationsverlauf treffen können.
- Trampelpfade. In einem Stadtplan sind sie in der Regel nicht eingezeichnet, werden aber trotzdem intensiv genutzt (sonst würden wir sie auf der Wiese gar nicht sehen). Sie entsprechen den ungeplanten, aber doch wiederkehrenden Kommunikationsprozessen in einem Unternehmen.

Beiden Systemen, dem Straßenverkehr wie der Unternehmenskommunikation, liegen Regeln und Anweisungen zugrunde. Was im Straßenverkehr die Straßenverkehrsordnung ist, ist in der Unternehmenskommunikation die Summe der Richtlinien, Anweisungen und Vorlagen für die Kommunikation.

Die Frage ist, welche dieser verschiedenen Kommunikationswege sich jetzt mit IT-Werkzeugen umsetzen lassen, und zwar so, dass sowohl die Kommunikationspartner als auch das Unternehmen davon profitieren.

2.2 Was sind Kommunikationsprozesse?

Wenn wir ein Unternehmen betrachten und im ersten Ansatz überlegen, wo überall Kommunikation stattfindet, können wir eine einfache Formel der Kommunikationsanalyse anwenden: Anzahl der Gesprächspartner x (Anzahl der Gesprächspartner – 1) / 2. Der Formel liegt die Annahme zugrunde, dass jeder im Unternehmen mit jedem reden kann, außer mit sich selbst. Hat ein Unternehmen also 250 Mitarbeiter, lautet die Formel 250 x 249 / 2 = 31125. Theoretisch bestehen hier also 31125 Kommunikationswege, die wir zu betrachten haben. Und darin sind die externen Kommunikationsbeziehungen noch nicht enthalten. Zum Glück ist diese Zahl eher als Indikator denn als konkrete Aufgabenstellung zu interpretieren. Sie gibt uns ein Verständnis von der Komplexität der Aufgabe, Kommunikation im Unternehmen zu gestalten.

In diesem Buch geht es nun aber um die Unterstützung der Kommunikation mit IT. Die erste Vermutung, die Sie sicherlich mit mir teilen, geht dahin, dass die IT-Unterstützung nicht bei allen möglichen Kommunikationsarten im Unternehmen und sicherlich auch nicht überall in gleicher Weise möglich oder auch nur wünschenswert ist. Ich behaupte aber, dass sie erstaunlicherweise bei mehr Kommunikationsarten möglich und auch sinnvoll ist, als man im ersten Schritt annehmen würde.

Klassischerweise wird von IT gesagt, sie spiele immer dann ihre Stärken aus, wenn wir einen Ablauf klar vordefinieren können. Ein einmal definierter Ablauf, der immer wieder in derselben Weise wiederholt werden kann, ist ein Prozess (im Gegensatz zu einem Projekt, bei dem der individuelle Ablauf immer wieder neu zu planen ist). Wir sollten uns also Gedanken darüber machen, wann wir Kommunikation als Prozess beschreiben können bzw. welche der Kommunikationsarten im Unternehmen tatsächlich als Prozesse definiert werden können, um sie dann entsprechend in der IT-Umgebung abbilden zu können.

2.2.1 Kommunikation als Prozess

Wie oben gesagt, ist ein Prozess ein wiederholbarer, vordefinierter Arbeitsablauf. Dieser Ablauf wird in der Regel beschrieben über die Eingaben in den Prozess, die Verarbeitungsschritte innerhalb des Prozesses und die Ausgabewerte aus dem Prozess. In der detaillierten Prozessanalyse bezieht man den Lieferanten bzw. die Herkunft der Eingabewerte und den Abnehmer der Ausgabewerte bzw. den Kunden in die Betrachtung mit ein. Diese Art der Beschreibung lässt sich als sogenanntes SIPOC-Diagramm darstellen (SIPOC steht für Supplier, Input, Process, Output und Customer) (vgl. Bild 2.1).

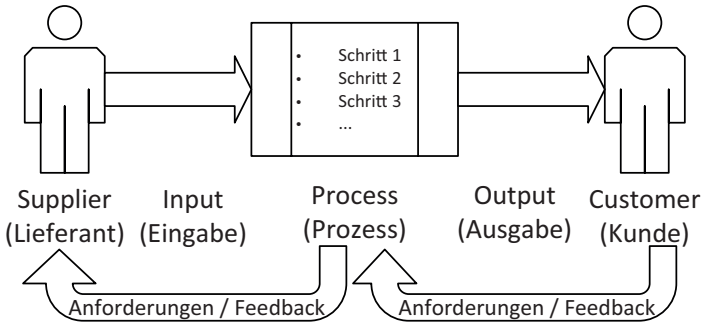

Bild 2.1 Das Prinzip eines SIPOC-Diagramms

Gerade für die Betrachtung unserer Kommunikationsprozesse bietet sich diese Darstellungsform an. Wie einleitend gesagt, ist der Kunde, oder besser der Empfänger unserer Kommunikation, eine der wichtigsten Stellen für die Prüfung des Erfolges. Nur wenn bei ihm die gewünschte Reaktion ausgelöst wird, ist unsere Kommunikation erfolgreich. Daher würde eine Betrachtungsweise, die mit dem „Output" endet, für die Gestaltung von Kommunikationsprozessen nicht ausreichen. Dass ein Kommunikationsprozess z. B. den Statusbericht eines Projekts auswirft sagt noch nichts darüber aus, ob der Prozess richtig angelegt ist. Erst wenn der Statusbericht die Informationen in einer Darstellung enthält, die der Lenkungsausschuss, der Kunde oder die Geschäftsführung für weitere Entscheidungen benötigt, können wir davon ausgehen, dass der Prozess das gewünschte Ergebnis liefert.

Ähnliches trifft auf Lieferantenseite in unserem Kommunikationsprozess zu. Diese stellt nämlich nicht einfach nur denjenigen dar, der den Prozess auslöst, sondern umfasst die Herkunft aller benötigten Informationen für den Start des Prozesses. Im Falle des oben genannten Statusberichts also die Fortschrittsinformationen aus dem Projektteam. Diese werden im Statusbericht des Projektleiters an den Lenkungsausschuss zusammengefasst. Ohne diese Informationen kann der Prozess nicht erfolgreich durchgeführt werden. Da diese Informationen in der Regel wieder aus anderen Kommunikationsprozessen kommen, erlangen wir über diese Betrachtung eine Gesamtdarstellung der Kommunikation im Unternehmen. Daraus ergibt sich somit die hier beschriebene Prozesslandschaft des Unternehmens.

Gleichzeitig können wir auf diesem Weg die Prozesse Schritt für Schritt vom Empfänger zurückbetrachten und damit klar die Anforderungen an die jeweilige Kommunikation definieren. Eine zentrale Entscheidung ist dabei die Festlegung der Prozessgrenzen. Indem wir festlegen, welches Ereignis wir als Start des Prozesses ansehen und welchen Zustand oder

welches Ereignis als Abschluss des Prozesses, definieren wir gleichzeitig den Bereich unserer Betrachtung. Wählen wir diesen zu eng, können wir wichtige Bedingungen und Eingabewerte übersehen, wählen wir ihn zu weit, kann es passieren, dass wir die entscheidenden Steuerungsfaktoren des Prozesses nicht isolieren können.

Veranschaulichen wir uns das am Beispiel des oben schon erwähnten Statusreporting im Projekt. Wir können den Prozess einerseits so beschreiben, dass er die Verarbeitung der Fortschrittsinformationen des Teams umfasst, das heißt der Prozess beginnt mit dem Eingang der Fortschrittsberichte des Teams. In der SIPOC-Beschreibung sieht das dann wie folgt aus (Tabelle 2.1):

Tabelle 2.1 Statusreporting als Gesamtprozess

Supplier	Input	Process	Output	Customer
Team	Fortschritts-informationen	Fortschritts-informationen zusammentragen	Statusbericht	Lenkungsausschuss, Geschäftsführung
Lieferanten		Bericht erstellen		
		Bericht versenden		

Bei dieser Art der Beschreibung wird der Verarbeitungsschritt, den der Projektleiter durchzuführen hat, die Analyse und die Zusammenfassung der Statusinformationen, nicht wirklich deutlich.

Im anderen Fall stellen wir den Gesamtprozess als zwei Prozesse dar, einmal das Fortschrittsreporting (Tabelle 2.2) des Teams und einmal das Statusreporting (Tabelle 2.3) des Projektleiters. Die Darstellungen sehen wie folgt aus:

Tabelle 2.2 Fortschrittsreporting

Supplier	Input	Process	Output	Customer
Team	Fortschritts-daten	Daten erfassen	Fortschritts-informationen	Projektleiter
Lieferanten		Bericht versenden		

Tabelle 2.3 Statusreporting

Supplier	Input	Process	Output	Customer
Projektleiter	Status-informationen	Status-informationen zusammentragen	Statusbericht	Lenkungsausschuss, Geschäftsführung
		Bericht erstellen		
		Bericht versenden		

In diesem Fall wird der Zusammenhang zwischen beiden Prozessen in der Darstellung nicht deutlich. Wir kommen also nicht umhin, uns ein weiteres Werkzeug zurechtzulegen, das diese Abhängigkeiten deutlich macht. Dies kann meines Erachtens am besten durch

eine Swimlane-Darstellung erfolgen. Dabei wird jede ausführende Stelle im Prozess durch eine eigene „Schwimmbahn“ dargestellt, in der die von dieser Stelle auszuführenden Prozessschritte beschrieben werden. Für unser Beispiel sieht eine solche Darstellung, wenn auch noch unvollständig, folgendermaßen aus (Bild 2.2):

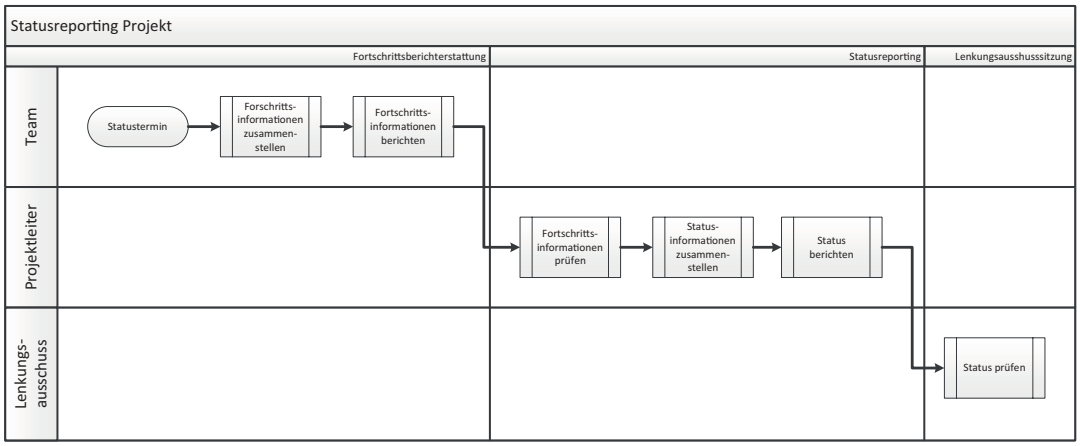

Bild 2.2 Der Reportingprozess als Swimlane-Diagramm

Hier wird deutlich, wie die einzelnen Prozesse und Prozessschritte auch funktionsübergreifend miteinander verzahnt sind. Daher eignet sich diese Darstellung am besten, um einen gesamten Prozessverlauf zu prüfen und zu planen. Die SIPOC-Darstellung ist dagegen eher geeignet, die einzelnen Prozessschritte detailliert zu analysieren.

Die Gesamtheit der Swimlane-Darstellung ergibt wiederum eine Repräsentation der Prozesslandschaft der Kommunikation im Unternehmen.

2.2.2 Externe und interne Kommunikationsprozesse

Eine erste grundlegende Unterscheidung der Kommunikationsarten im Unternehmen betrifft die Stellung der Kommunikationspartner zum Unternehmen, also ob sie als Mitarbeiter Teil des Unternehmens sind oder ob sie nicht zur Unternehmensorganisation gehören, wie z. B. Kunden oder Lieferanten. Von internen Kommunikationsakten sprechen wir, wenn beide Kommunikationspartner Bestandteil der Organisation selbst sind, z. B. der Mitarbeiter und sein Vorgesetzter im Personalgespräch. Externe Kommunikation meint die Kommunikation mit Kommunikationspartnern außerhalb des Unternehmens, beispielsweise das Angebot für eine Leistung an einen Kunden. Warum ist diese Unterscheidung in unserer Betrachtung von Bedeutung?

Die wichtigste Auswirkung besteht in der Tatsache, dass in der Kommunikation mit nicht zur Organisation gehörenden Kommunikationspartnern nicht die Person eigentlicher Absender oder Adressat einer Äußerung ist, sondern das Unternehmen selbst. Ein Angebot an einen Kunden ist kein Angebot eines Vertriebsmitarbeiters des Unternehmens, sondern ein Angebot des Unternehmens an seinen Kunden. Für die Erfüllung der Leistung muss das Unternehmen einstehen, nicht der einzelne Vertriebsmitarbeiter.

Aus dieser einfachen Tatsache leiten sich eine Reihe von Anforderungen an die Gestaltung der Kommunikation her, die wir bei der Planung der Prozesse zu berücksichtigen haben. Diese sind unter anderem, aber nicht ausschließlich, die folgenden:

- Die Äußerung muss deutlich machen, dass hier das Unternehmen spricht.
- Die rechtliche Verbindlichkeit der Aussage muss berücksichtigt werden.
- Der Wahrung des Unternehmensimages muss Genüge geleistet werden.

Aufgrund dieser, aus Unternehmenssicht relevanter Anforderungen sind externe Kommunikationsprozesse in der Regel deutlich strikter zu gestalten als interne Prozesse. Die Einhaltung der Anforderung wird über die Kombination mehrerer Verfahren versucht sicherzustellen. So werden für externe Kommunikationsakte sehr häufig Vorlagen verwendet, von einfachen Briefvorlagen bis hin zu komplexen Dokumentvorlagen. Diese Vorlagen unterliegen strengen Designvorgaben, über die auch das Unternehmensimage transportiert wird. Häufig gibt es auch Formulierungsvorgaben, bis hin zu Textbausteinen. In die Prozesse werden Prüfungs- und Genehmigungsschritte eingebaut, die zumindest die Einhaltung eines Vier-Augen-Prinzips sicherstellen sollen. Darüber hinaus kommen Dokumentations- und Archivierungsverfahren zum Einsatz, die die Nachvollziehbarkeit gewährleisten sollen. Diese Aufzählung ließe sich weiter fortsetzen, soll aber für den gegenwärtigen Diskussionsstand ausreichen.

Wenn wir uns also in der Folge damit beschäftigen, wie wir externe Kommunikationsakte in unseren IT-Werkzeugen abbilden können, müssen wir schon bei der Auswahl der Werkzeuge berücksichtigen, dass entsprechende Funktionen vorhanden oder zumindest integrierbar sind.

Auch wenn die interne Kommunikation häufig unter weniger strikten Vorgaben geplant wird, sind auch hier einige Faktoren zu berücksichtigen. Insbesondere die einfache Integration in den Arbeitsprozess spielt hier eine große Rolle. Kommunikation im Unternehmen soll in der Regel zeitnah und schnell erfolgen. Das heißt, der Mitarbeiter sollte sie aus seiner normalen Arbeit heraus durchführen können, ohne dafür spezielle Werkzeuge auswählen zu müssen oder für die verschiedenen Kommunikationsarten zwischen verschiedenen Werkzeugen wechseln zu müssen. Um die Prozesse einfach und die Information konsistent zu halten, sollten möglichst keine Medienwechsel erforderlich sein. Die beste interne Kommunikation findet statt, wenn sie sozusagen en passant passiert.

Wenn ein Vertriebsmitarbeiter z. B. seinen Vorgesetzten darüber informieren will, dass er eine neue Kalkulation für ein Projektangebot gemacht hat, kann er das natürlich machen, indem er die in Excel erstellte Kalkulation per E-Mail an seinen Vorgesetzten schickt.

Dazu muss er aber schon mehrere Schritte ausführen, das Speichern der Kalkulation, das Erstellen der E-Mail, das Anhängen der Datei und das Versenden der E-Mail. Bei jedem dieser Schritte können Fehler auftreten, er kann die falsche Datei anhängen, kann den falschen Empfänger auswählen etc. Wenn er jetzt nicht nur seinen Vorgesetzten, sondern auch andere Beteiligte informieren möchte, sieht das auf den ersten Blick nicht komplizierter aus, da er einfach nur zusätzliche Empfänger in die E-Mail einträgt. Allerdings hat dann jeder Empfänger tatsächlich eine eigne Version der Datei, was bei Änderungen wieder zusätzliche Fehlerquellen ermöglicht und die Synchronisation dieser Änderungen aufwendig macht.

Wenn aber die Datei nun an einem Speicherort abgelegt wird, der so konfiguriert ist, dass alle Beteiligten automatisch verständigt werden und Änderungen nur an dieser Stelle, der einen abgelegten Datei, durchgeführt werden, reduziert sich sowohl der Aufwand als auch die Fehlerträchtigkeit des Verfahrens erheblich. Meines Erachtens ist es daher erstaunlich, dass selbst große Unternehmen häufig noch nach dem ersten Verfahren arbeiten, obwohl wir heute einfache Technologien zur Verfügung haben, die das zweite Verfahren unterstützen.

2.2.3 Horizontale und vertikale Kommunikationsprozesse

Neben der Integrierbarkeit in den Arbeitsprozess ergeben sich für einige interne Kommunikationsprozesse noch spezielle Anforderungen, die sich aus der Struktur eines Unternehmens herleiten. Unternehmen sind auch heute noch in den meisten Fällen hierarchisch strukturierte Organisationen. Viele (wenn auch nicht alle) interne Kommunikationsprozesse folgen dieser Struktur, entweder weil sich die Kommunikationspartner auf derselben Hierarchieebene befinden oder weil genau dies nicht der Fall ist. Im ersten Fall spricht man von horizontaler Kommunikation, da der Kommunikationsprozess im Organigramm des Unternehmens als waagrechte Linie dargestellt werden könnte, im zweiten Fall von vertikaler Kommunikation, da er im Organigramm eine senkrechte Linie bilden würde (vgl. Bild 2.3).

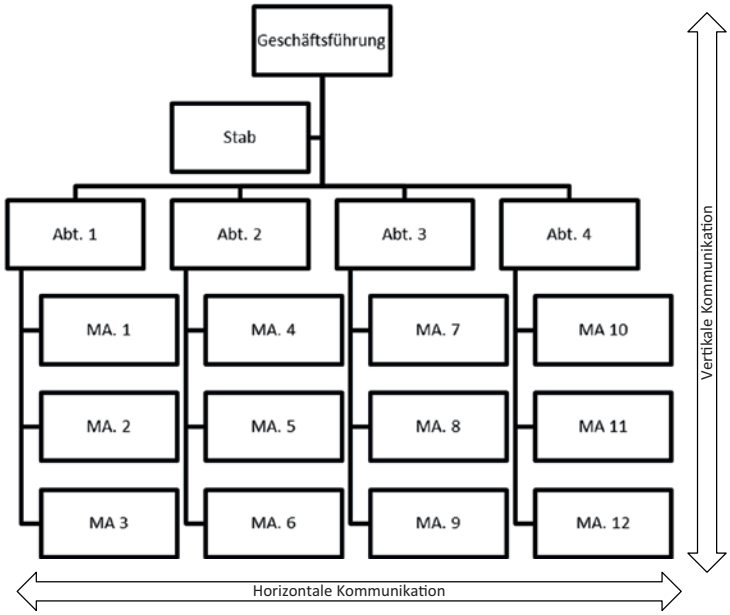

Bild 2.3 Vertikale und horizontale Kommunikation im Unternehmen

Typische horizontale Kommunikationsakte sind z. B. die Abstimmung komplexer Angebote über mehrere Abteilungen, die Weitergabe von Rechnungsinformationen an die Buchhaltung oder Ähnliches.

Beispiele für vertikale Kommunikationsprozesse sind das Finanzreporting für den Jahresabschluss, die Weitergabe von Budgetplanungen der Abteilung an den Geschäftsbereich oder einfach die Eskalation von Entscheidungsprozessen.

Gerade die Reportingprozesse zeigen die besonderen Anforderungen an viele vertikale Kommunikationsprozesse. Viele dieser Prozesse sind nämlich mit Aggregationsverfahren verknüpft, denen der Kommunikationsprozess Rechnung tragen muss. Das heißt die Informationen, die aus einem solchen Kommunikationsakt weitergegeben werden, müssen mit den Informationen aus dem gleichen Kommunikationsakt einer anderen Stelle zusammengefasst werden können oder zumindest vergleichbar sein. Auf der obersten Hierarchieebene des Unternehmens müssen die entsprechenden Informationen zu einem Gesamtüberblick zusammengefasst werden können. Es würde z. B. wenig Sinn machen, wenn die eine Abteilung ihren Finanzbedarf für die nächsten fünf Jahre meldet, ohne ihn weiter aufzuteilen, und eine andere den Finanzbedarf für ein Jahr meldet, wenn das Unternehmen einen Planungshorizont von zwei Jahren ermitteln möchte.

Bei der Gestaltung vertikaler Kommunikationsprozesse müssen wir also Werkzeuge finden, die die einfache Aggregierbarkeit gewährleisten können. Darüber hinaus müssen wir die Prozesse so planen, dass tatsächlich nur vergleichbare Daten geliefert werden können.

Sie mögen jetzt vielleicht einwenden, dass diese Sichtweise der heutigen Unternehmenswirklichkeit nicht mehr ganz gerecht wird, da moderne Unternehmen doch nicht mehr strikt in hierarchischen Strukturen arbeiten. Da gebe ich Ihnen Recht. Schon seit einiger Zeit versuchen Unternehmen bewusst, diese hierarchische Strukturierung aufzulösen und vernetzt zu arbeiten. Ausdruck dieser Tendenz ist der hohe Anteil an projektbasierter Teamarbeit im Unternehmen. Teams überschreiten in der Regel die hierarchischen Grenzen und bestehen aus Mitarbeitern unterschiedlicher Hierarchieebenen und Abteilungen. Das heißt zwar nicht, dass es keine horizontalen und vertikalen Kommunikationsakte im Unternehmen mehr gibt, es heißt aber, dass wir noch weitere Kommunikationsrichtungen zu berücksichtigen haben, die weniger gerichtet sind. Meines Erachtens kann man diese am besten als vernetzte Kommunikation bezeichnen. Aus den Ansätzen des Wissensmanagements kennt man den großen Vorteil der vernetzten Arbeitsweise für eine schnelle und umfassende Kommunikation im Unternehmen: Wissen verbreitet sich schneller, neues Wissen kann schneller aufgebaut werden und die Innovationskraft des Unternehmens wird dadurch gestärkt – in der heutigen Zeit ein nicht zu unterschätzender Erfolgsfaktor.

Damit das aber funktioniert, sind auch hier Kommunikationswerkzeuge zu planen, die diese Art der Kommunikation unterstützen. Dazu wird heute sehr häufig auf die Ansätze zurückgegriffen, die sich im sogenannten Web 2.0 in Form sozialer Netzwerke entwickelt haben. Viele Plattformen bieten auch dafür unternehmensinterne Möglichkeiten. Allerdings stellt auch hier die Unternehmensumgebung Anforderungen, die sich gerade aus der Schnelligkeit und dem Wunsch, mit dem Wissen im Unternehmen bewusst umzugehen, herleiten.

Diese Kommunikation muss ebenso einfach und schnell erfolgen können, wie andere interne Kommunikationsprozesse. Sie muss aber darüber hinaus auch bei wenig Struktur eine gute Wiederauffindbarkeit aufweisen. Wenn Informationen in weniger strukturierten Umgebungen gespeichert werden, wird es schwieriger, die richtigen Informationen schnell zu finden. Wenn das wiederum nicht möglich ist, werden die Informationen nicht genutzt. Häufig ergibt sich dieses Dilemma daraus, dass die Kriterien, die bei der Ablage der Infor-

mationen zur Strukturierung angewendet werden, andere sind als die, die bei der Suche eine Rolle spielen. Dies ist ein Effekt, den man aus vielen Wissensmanagementprojekten kennt. Das hat auch damit zu tun, dass die Zeitpunkte zwischen der Speicherung und der Nachfrage teilweise weit auseinanderliegen, wir es also mit einem asynchronen Kommunikationsprozess zu tun haben. Damit wollen wir uns im folgenden Abschnitt beschäftigen.

Am besten arbeiten solche netzwerkorientierten Plattformen, wenn die Information tatsächlich nicht explizit klassifiziert werden muss, sondern sich die Klassifizierung aus der Art der Information selbst ergibt. Dafür benötigen die Plattformen aber Rahmeninformationen in Form sogenannter Ontologien, das heißt eine Vorstrukturierung möglicher Arten von Informationen. Man kann sich das an den sozialen Netzwerken einfach vor Augen halten. Wenn Sie in einem solchen Netzwerk etwas posten, entscheidet das Netzwerk selbständig, für wen das interessant ist und bietet diese Informationen an. Dies passiert z. B. dadurch, dass aus dem Post Ortsinformationen ausgelesen werden, die den Inhalt für Personen am selben Ort interessant machen, oder indem sie auf etwas verweisen, nach dem auch andere häufig nachgefragt haben. Das System benötigt dafür Informationen über die Geografie Ihrer Umgebung, um zu wissen, wer sich in Ihrer Nähe befindet. Das ist ein Teil einer Ontologie.

Wenn wir also nach Möglichkeiten suchen, solche Kommunikationsprozesse im Unternehmen technologisch zu unterstützen, müssen wir Werkzeuge auswählen, die Analyse- und Suchfunktionen mit der Möglichkeit verbinden, Ontologien des Unternehmens zu erstellen, also eine Klassifizierung der Unternehmensumwelt vornehmen können. Dies können im einfachen Falle vordefinierte Dokumentenklassen sein.

2.2.4 Synchrone und asynchrone Kommunikation

Nicht immer findet Kommunikation als ein Prozess statt, in dem die beteiligten Kommunikationspartner zur selben Zeit interagieren. Insbesondere wenn wir uns vertikale Kommunikationsprozesse im Unternehmen anschauen, werden wir häufig den Effekt finden, dass es keine direkte Interaktion zwischen den Kommunikationspartnern gibt. Dabei handelt es sich häufig um informierende Kommunikationsprozesse, deren Zweck darin besteht, dem Empfänger die Möglichkeit zu geben, auf vorhandenes Wissen zuzugreifen, ohne aber eine direkte Reaktion von ihm zu erwarten. Es ist z. B. nicht schwierig, sich darunter Dokumentationsprozesse vorzustellen. Sehr häufig spielen diese Prozesse daher auch im Umfeld des Wissensmanagements eines Unternehmens eine Rolle.

Ein gutes, wenn auch vielleicht extremes Beispiel für einen solchen asynchronen Prozess sind die an amerikanischen Schulen sehr beliebten Zeitkapseln. Dabei werden Briefe von Schülern und andere Dinge in Edelstahlbehälter gepackt und diese dann z. B. eingegraben oder in Fundamente von Schulneubauten in Beton eingegossen. Ziel ist es, zukünftigen Generationen Informationen und Erkenntnisse über die heutige Zeit zu liefern, z. B. wenn das Schulgebäude in hundert Jahren abgerissen wird und dabei die Zeitkapsel zum Vorschein kommt. Es ist natürlich nicht ganz richtig, dass wir dann keine Reaktion vom Empfänger erwarten. Die Schüler stellen sich sicherlich schon vor, wie die Menschen auf ihre Briefe reagieren, wenn sie diese finden. Die Reaktion selbst hat aber keine Auswirkungen auf uns selbst, da sie zu einer Zeit stattfinden wird, in der wir nicht mehr existieren.

Im Unternehmen sind für diese Prozesse zwei Hauptanforderungen von Bedeutung. Zum ersten natürlich die reine Speicherbarkeit und Dauerhaftigkeit der Information bzw. der Äußerung selbst (die natürlich nicht immer nur sprachlich sein muss). Zum anderen aber auch die Sicherstellung der Interpretierbarkeit. Das heißt, die Daten müssen so gespeichert werden, dass später daraus noch die richtigen Informationen gelesen werden können.

Gerade dieser letzte Aspekt ist aus Sicht der Kommunikationsplanung von großer Bedeutung. In Ermangelung der direkten Interaktion können wir Missverständnisse nicht in der Kommunikation behandeln, sondern müssen diese vorausplanen. Auch hat der Empfänger bei einem größeren Zeitversatz häufig keine Möglichkeit nachzufragen, sondern kann die Informationen nur aus seinem eigenen Kontext heraus interpretieren. Da in der Kommunikation allgemein der Satz gilt, dass der Sender dafür verantwortlich ist, die Äußerung so zu gestalten, dass sie vom Empfänger richtig verstanden wird, müssen wir versuchen, den Kontext möglichst genau vorauszuplanen bzw. möglichst viel Kontext mitzuliefern, um das richtige Verständnis sicherzustellen.

In der Praxis heißt das, dass asynchrone Kommunikationsprozesse expliziter gestaltet werden müssen. Besonders in den Fällen, in denen asynchrone Kommunikation mit der Aggregation von Informationen zusammenfällt, also z. B. im klassischen Unternehmensreporting, empfinden wir diese beiden häufig als widerstreitende Anforderungen. Damit Informationen zusammengefasst werden können, müssen wir abstrahieren. Mit der Abstraktion geht aber gleichzeitig der Kontext verloren. Wir haben dann häufig das Gefühl, nicht genügend Informationen liefern zu können und empfinden unsere Aussage dann nicht richtig beurteilt. Diesen Effekt sollten wir bei der Gestaltung asynchroner Kommunikation im Blick behalten.

2.3 Anforderungen an (Unternehmens-) Kommunikation

Wenden wir unsere einleitend erläuterte Sichtweise also auf die Kommunikation im Unternehmen an und versuchen dabei zu ermitteln, welche weiteren Einflussfaktoren deren Erfolg bestimmen.

2.3.1 Verständlichkeit

Auch wenn es sich nach einer Banalität anhört, in der Betrachtung von Kommunikation von Verständlichkeit zu reden, lohnt es sich doch, einen genaueren Blick darauf zu werfen, wie wir sicherstellen können, dass wir richtig verstanden werden. Zunächst einmal müssen wir die verschiedenen Aspekte des Begriffs klarstellen. Verständlichkeit kann sich nämlich auf mehrere Seiten der Kommunikation beziehen.

Einmal ist damit die physische Ebene angesprochen, also die Tatsache, dass unsere Kommunikation überhaupt wahrgenommen wird. Wenn wir sprechen, muss unser Gegenüber uns hören können. Geht unsere Äußerung im Umgebungslärm unter oder kann nicht klar davon

unterschieden werden, werden wir nicht verstanden. In der Kommunikationsplanung spielt dieser Aspekt insbesondere in der Auswahl des Kommunikationsmediums eine Rolle. Die richtige Auswahl des Mediums stellt sicher, dass unsere Nachricht auch ankommt. Akustische Medien, soweit sie nicht elektronisch vermittelt werden, haben nur eine begrenzte Reichweite. Daher wurden auf See die Flaggensignale eingeführt, also ein visuelles Medium, das über größere Entfernungen wahrgenommen werden kann.

Für die Kommunikationsplanung ergibt sich die Auswahl des Mediums aber auch aus den später zu betrachtenden nicht-funktionalen Anforderungen wie Zuverlässigkeit, Verfügbarkeit und Sicherheit.

Die zweite Ebene, auf die sich die Verständlichkeit beziehen kann, ist die inhaltliche Ebene, also die Möglichkeit des Empfängers, den Inhalt der Nachricht zu erfassen. In der Kommunikationsanalyse kennen wir dafür den Begriff der Decodierung. Hier spielt z. B. die ausgewählte Sprache eine große Rolle. Gerade in internationalen Unternehmen werden kommunikative Kernprozesse häufig in einer für das Unternehmen festgelegten Standardsprache wie Englisch durchgeführt. Damit das funktioniert, müssen natürlich alle Kommunikationspartner über ausreichende Sprachkenntnisse verfügen. Das Risiko von Missverständnissen ist aber auch dann vorhanden, wenn dieselben Prozesse in verschiedenen Sprachen durchgeführt werden, zumindest wenn die Ergebnisse wieder aggregiert werden müssen. Es verschiebt sich nur auf die Ebene der Aggregation, da hier sichergestellt werden muss, dass die Ergebnisse vergleichbar sind.

Darüber hinaus spielen aber auch andere Aspekte für das inhaltliche Verständnis eine Rolle, nämlich das Umgebungswissen, wie z. B. das Wissen über die Verwendung spezifischer Ausdrücke im Unternehmen oder die Kenntnisse der Strukturen, in denen die Kommunikation stattfindet. In der Kommunikationsplanung können wir uns die im Abschnitt 2.2.3 angesprochenen Ontologien zunutze machen. Durch Festlegung von Begriffen und anderen Elementen in einer Ontologie und durch den Verweis auf diese Ontologie in der Kommunikation können wird die einheitliche Verwendung und ein einheitliches Verständnis sicherstellen. Wenn wir z. B. eine vordefinierte Liste von Unternehmensbereichen als Auswahlfeld in einem Formular verwenden, ist sichergestellt, dass dieselben Unternehmensbereiche auch über dieselben Namen angesprochen werden. Damit bilden wir einen Teil des Umgebungswissens ab, den sonst der Benutzer selbst einbringen müsste. Im letzten Fall besteht dabei immer die Gefahr, dass gleiche Dinge unterschiedlich bezeichnet werden oder unterschiedliche Dinge mit ähnlichen Begriffen belegt werden, was zu Missverständnissen führen kann.

Diese Ebene der Verständlichkeit hat direkte Auswirkungen auf die Planung unserer Kommunikationsprozesse, da natürlich sichergestellt werden muss, dass die Inhalte auch richtig verstanden werden. In der Regel versuchen wir das über die Formalisierung der Prozesse zu erreichen. Formalisierte Sprachen wie z. B. die Mathematik gelten als eindeutiger als weniger formalisierte Kommunikationsmethoden. Der Begriff „formalisiert“ deutet schon an, dass wir dazu in der Kommunikation mehr oder weniger strikt vorgegebene Formulare verwenden. Ein Formular zeichnet sich dadurch aus, dass die einzelnen inhaltlichen Bestandteile klar definiert sind und nur in einer vordefinierten Form (in einem Formularfeld) angegeben werden können.

In weniger formalisierten Prozessen können wir das Verständnis absichern, indem wir einen offenen Feedbackkanal haben, das heißt einen Weg, über den wir nachfragen und

Einzelaspekte abklären können. Wir können dazu z. B. auch freie Kommentarfelder in Formularen nutzen.

Die dritte Ebene, auf die sich der Begriff Verständlichkeit bezieht, ist die Handlungsebene. Damit ist gemeint, dass der Kommunikationspartner versteht, welche Reaktion von ihm erwartet wird bzw. was er mit der übermittelten Information machen soll. Dieser Aspekt hat für die Unternehmenskommunikation mindesten ebenso viel Bedeutung wie der inhaltliche. Kommunikationsprozesse dienen in der Regel dazu, Aktionen im Unternehmen auszulösen. In stark standardisierten Prozessen stellt das auf den ersten Blick kein Problem dar, da die Aktion direkt mit dem Kommunikationsergebnis gekoppelt werden kann. Wenn also z. B. die Freigabe eines Dokumentes angefordert wird, kann der Prozess so angelegt werden, dass die Nachricht selbst schon einen Verweis auf die Aktion, z. B. in Form eines Links oder einer Schaltfläche, enthält. Trotzdem gibt es auch hier immer wieder Missverständnisse in der Kommunikation. Das ist z. B. der Fall, wenn der Empfänger aus der Nachricht nicht entnehmen kann, dass er das Dokument vorher zu prüfen hat und dieser Prozess neu für ihn ist, er es daher aus seinem Wissen auch nicht erschließen kann.

Gerade für das Handlungsverständnis der Kommunikation spielen wiederum kulturelle Aspekte eine Rolle. Aspekte wie Höflichkeit, Hierarchiedenken, Verantwortungsgefühl etc. sind in verschiedenen Kulturen häufig mit unterschiedlichen Mitteln und in unterschiedlicher Ausprägung kommunikativ umgesetzt. Das betrifft nicht nur die Kulturen verschiedener Länder, sondern kann auch schon zwischen Unternehmen und sogar innerhalb eines Unternehmens zwischen Abteilungen auftreten. Im Extremfall kann das dazu führen, dass erforderliche Kommunikationsprozesse des Reportings nicht durchgeführt werden, weil sie nicht als Weitergabe von Informationen verstanden werden, sondern als Schuldbekenntnis für Fehler interpretiert werden. In international arbeitenden Unternehmen finden sich dafür immer wieder Beispiele.

Der Handlungsaspekt spielt im kommunikativen Verständnis aber auch zwischen Individuen eine große Rolle. Dem Leser ist womöglich das Vier-Ohren-Modell von Friedemann Schulz von Thun ein Begriff[1]. Schulz von Thuns Ansatz, und mit ihm viele andere psychologische Ansätze, machen deutlich, dass eine Äußerung immer unter verschiedenen Handlungsaspekten verstanden werden kann und es von der Situation, den beteiligten Personen, der Form der Äußerung und verschiedenen anderen Aspekten abhängt, welcher der Aspekte in den Vordergrund tritt. Bei Schulz von Thun sind das der inhaltliche und der Beziehungsaspekt, der Appell und die Kundgabe. Eine Äußerung wie „Mir ist kalt“ kann demnach vier verschiedene Reaktionen hervorrufen, je nachdem welcher Aspekt beim Hörer wirksam wird (Schulz von Thun spricht dabei von den vier Ohren des Hörers): „Ja, ich glaube, es sind nur 15 Grad Celsius hier“ (Inhalt), „Sie Ärmster, das tut mir Leid“ (Kundgabe), „Okay, ich mache das Fenster zu“ (Appell), „Mach dein Fenster doch selber zu, ich bin nicht dein Diener“ (Beziehung).

Spielen diese Aspekte in unseren Kommunikationsprozessen auch eine Rolle? Ich meine ja, da auch prozessgebundene Kommunikation immer noch Kommunikation ist und daher auch entsprechend von uns interpretiert wird. Das heißt ein Prozess, der uns z. B. auffordert, Fehler zu berichten, kann leicht auf dem Beziehungsaspekt missverstanden und dann

[1] (Friedemann Schulz von Thun: Miteinander Reden 1: Störungen und Klärungen. Allgemeine Psychologie der Kommunikation, Reinbek bei Hamburg 1981)

so ausgeführt werden, dass er nicht das gewünschte Ergebnis bringt, also ein ehrliches Reporting. Nicht alle Faktoren, die darauf Einfluss haben, lassen sich aber im Unternehmen steuern. Zumindest aber formale Faktoren, wie die Art der Aufforderung, und gewisse kulturelle Faktoren, wie z. B. der Umgang mit offenen Äußerungen, lassen sich aber gestalten. Auch das grundlegende Handlungsverständnis können wir dadurch absichern, dass im Prozess deutlich wird, was als Handlung erwartet wird bzw. welche Reaktionen erfolgen werden. Das hat auch viel mit unserem nächsten Aspekt, der Nachvollziehbarkeit der Prozesse, zu tun.

2.3.2 Integrität/Nachvollziehbarkeit

Die Nachvollziehbarkeit bzw. Integrität eines Kommunikationsprozesses bezieht sich ebenfalls auf zwei Aspekte. Einerseits ist es, wie im vorigen Abschnitt angesprochen, für den auslösenden Kommunikationspartner wichtig zu wissen, welche Auswirkungen seine Kommunikation hat. Er muss also den Prozess verstehen und wissen, warum und mit welchem Ziel er kommuniziert. Wenn ich jemanden informieren soll, muss ich wissen, warum derjenige die Information benötigt und was er mit der Information anfangen wird. Nur dann kann ich entscheiden, wie ich sie am besten übermittle und ob ich dafür den richtigen Weg ausgewählt habe.

Auf der Empfängerseite ist aber auch der Aspekt der Nachvollziehbarkeit von Bedeutung. Damit der Empfänger die Äußerung richtig einschätzen kann, muss er wissen, woher sie kommt. In Unternehmen muss darüber hinaus auch noch sichergestellt sein, dass sie tatsächlich von der angegebenen Stelle kommt. In der IT kennen wir die Gefahr des Spoofing, das heißt des Vortäuschens eines falschen Absenders. Da Kommunikationsprozesse im Unternehmen, wie schon gesagt, Aktionen auslösen, muss sichergestellt sein, dass diese Aktion berechtigterweise ausgelöst wird.

Technisch setzen wir das in der Regel so um, dass wir einerseits auf eine sichere und nachvollziehbare Authentifizierung des Absenders setzen und andererseits auf Basis der Authentifizierung eine Autorisierung aufbauen, die sicherstellt, dass nur berechtigte Absender bestimmte Prozesse nutzen können. Wir benötigen also Sicherheitsmechanismen in unseren Kommunikationswerkzeugen, die beides durchführen können, die Authentifizierung und die Autorisierung. Dies wird umso wichtiger, je größer das Unternehmen ist, da sich dann die Kommunikationspartner nicht mehr von Person zu Person kennen.

In formalisierten Prozessen können wir das voraussichtlich besser umsetzen als in weniger formalen Kommunikationsarten. Eine einfache E-Mail mit einem angehängten Dokument kann von einem beliebigen Absender an mich gesendet werden. Ich kann in der Regel nur anhand der Absenderadresse ermitteln, ob er zu meinem Unternehmen gehört. Eventuell kann ich dann noch feststellen, in welcher Abteilung und in welcher Position er sitzt. Wenn der Einstieg in den Prozess aber schon eine Authentifizierung und Autorisierung erfordert, z. B. weil das Empfangspostfach so eingeschränkt ist, dass nur bestimmte Absender dahin versenden dürfen, besteht eine größere Sicherheit, dass die E-Mail berechtigterweise an mich gesendet wurde.

2.3.3 Zuverlässigkeit

Während wir bisher eher mit funktionalen Anforderungen an unsere Kommunikation zu tun hatten, sind die nächsten drei eher als nicht-funktionale Anforderungen einzustufen. Zuverlässigkeit ist eine davon. In der IT kennen wir diese auch unter den Begriffen der Verfügbarkeit oder Ausfallsicherheit einer Anwendung.

Von einem Kommunikationsprozess erwarten wir, dass er bis zum Ende durchgeführt wird, wenn wir ihn anstoßen. Wenn ich also die Quartalszahlen meiner Abteilung berichte, erwarte ich, dass diese auch in den entsprechenden Auswertungen ankommen. Häufig sind entsprechende Prozesse auch zeitkritisch, das heißt die Informationen müssen nicht nur ankommen, sondern dies auch zum richtigen Zeitpunkt. Nicht zu vergessen, dass sie auch an der richtigen Stelle ankommen müssen.

All diese Punkte fassen wir unter der Zuverlässigkeit der Kommunikationsprozesse zusammen. Die rein technischen Aspekte werden in der Regel durch die Infrastrukturplanung vorgegeben. Dass wir also eine ausfallsichere Gestaltung unserer Serverinfrastruktur, meistens in Form von Redundanz, auf verschiedenen Ebenen haben, ist kein Aspekt, den wir bei der Betrachtung unserer Kommunikationsprozesse explizit berücksichtigen werden. Wir sollten aber wissen, welchen Grad an Zuverlässigkeit wir haben, um in der Planung zu berücksichtigen, wie wir mit Ausfällen in unserer Kommunikation umgehen. Ob wir z. B. alternative Kommunikationswege bei zeitkritischen Kommunikationen vorsehen oder ob wir bewusst Feedbackkanäle einplanen, wenn erwartete Kommunikationsprozesse nicht zur rechten Zeit durchgeführt werden. Feedback heißt im einfachen Fall nachzufragen, wo denn die Zahlen bleiben.

2.3.4 Verfügbarkeit

Verfügbarkeit kann einerseits, wie im vorigen Abschnitt geschildert, auf die zeitliche Verfügbarkeit einer Anwendung bezogen werden. Andererseits heißt Verfügbarkeit aber auch: Können die Kommunikationspartner den Prozess, da wo sie sind, nutzen, das heißt steht er unter den erforderlichen Bedingungen zur Verfügung? Gerade in den Zeiten des mobilen Arbeitens mit Geräten wie Smartphones und Tablet-Computern gewinnt dieser Aspekt zunehmend an Bedeutung.

Während es heute üblich ist, über sein Smartphone auch per E-Mail zu kommunizieren, sieht das bei formalisierten Prozessen anders aus. Diese setzen häufig auf spezielle Anwendungen auf, für die ursprünglich nur die Eingabe per Computer vorgesehen war. Bei den großen Anbietern finden wir zwar in der Regel schon Apps für die Serveranwendungen. Da aber die Betriebssysteme bei den Smartphones anders verteilt sind, steckt dahinter ein nicht unerheblicher Entwicklungsaufwand. Außerdem ist zu bedenken, dass wir ja auch die Nachvollziehbarkeit der Kommunikation sicherstellen müssen. Je mobiler die Geräte sind, desto schwieriger gestaltet sich das. Die Authentifizierung wird in der Regel über das Gerät vorgenommen. Wenn dieses dann in die Hände eines unternehmensfremden Benutzers kommt, kann dieser theoretisch die Aktionen so ausführen, als sei er der ursprüngliche Besitzer des Gerätes.

Ein weiterer Aspekt spielt hier eine Rolle. Mobilität hat zur Folge, dass wir nicht immer mit dem Unternehmen verbunden sind, z. B. wenn kein Mobilfunknetz verfügbar ist. Die Frage

ist dann, bis zu welchem Grad einzelne Kommunikationsprozesse auch in einem solchen Fall arbeiten müssen. Müssen bestimmte Informationen als Ergebnisse von Kommunikationsprozessen auch ohne Verbindung zum Unternehmensnetz abfragbar sein? Oder müssen Kommunikationsakte auch offline ausgelöst werden können, auch wenn sie erst später verarbeitet werden? An diesen Fragestellungen sieht man schon, dass dieser Aspekt viel mit der asynchronen Gestaltung von Prozessen zu tun hat. Wobei die Asynchronizität auf beiden Seiten des Kommunikationsaktes auftreten kann.

2.3.5 Sicherheit und Vertraulichkeit

Vertrauliche Informationen liegen in Unternehmen an vielen Stellen vor, von den Gehaltsinformationen der Mitarbeiter über die Inhalte von Mitarbeitergesprächen bis hin zu technischen und strategischen Informationen der Produktentwicklung und den Inhalten von Kundenverträgen. Auch diese Informationen entstehen durch Kommunikation und werden in Kommunikationsprozessen weitergegeben und weiterverarbeitet. Vertraulichkeit heißt dabei, dass diese Informationen vor dem unberechtigten Zugriff und vor der unberechtigten Weitergabe geschützt werden müssen. Diesen Schutz stellen wir in der Regel über Sicherheitsmechanismen auf den verschiedenen Ebenen her.

Auf der organisatorischen Ebene kennen wir hier vertragliche oder ähnliche Vereinbarungen, die die Weitergabe von Informationen sanktionieren, wie z. B. Non-Disclosure-Agreements (NDA) oder Letter Of Intent (LOI).

Technisch kennen wir eine ganze Reihe von Mechanismen, die wir nutzen können. Das fängt bei den schon erwähnten Authentifizierungsmechanismen an und geht über Verschlüsselungsmechanismen bis hin zu Datenverkehrsüberprüfungen auf Firewalls und Proxyservern. Neben der Fragestellung, welche Mechanismen dabei von unserer Infrastruktur unterstützt werden und welche technischen Voraussetzungen wir dafür benötigen, werden wir bei der Planung unserer Kommunikationsprozesse insbesondere der Frage nachgehen, inwieweit wir entsprechende Sicherheitsmechanismen regelbasiert abbilden können, z. B. auf Basis der Identität der Kommunikationspartner oder des Inhalts der Kommunikation.

Gerade bei dem Aspekt der Sicherheit zeigt die Erfahrung aber immer wieder, dass alle technischen Möglichkeiten nie eine vollständige Sicherheit garantieren können, sondern dass dazu immer auch ein fundiertes Verständnis der Kommunikationspartner gehört. Es macht z. B. wenig Sinn, wenn wir die telefonische Kommunikation unserer Vertriebsmitarbeiter mit starken Verschlüsselungsmechanismen verschlüsseln, diese dann aber ihre Kundenverhandlungen per Telefon im Großraumwagen eines ICE führen. Möglichst noch auf der Rückfahrt von einer Fachtagung, auf der auch die Mitarbeiter des Wettbewerbs teilgenommen haben und eventuell im gleichen Wagen zurückfahren.

2.3.6 Flexibilität

Wir haben im Abschnitt 2.2.1 gesehen, dass Prozesse grundsätzlich die Eigenschaften haben, immer wieder in gleicher Weise wiederholt werden zu können und dabei das gleiche Ergebnis liefern. Daher scheint es auf den ersten Blick widersprüchlich, von einem Prozess

Flexibilität zu verlangen. Diese widerspricht ja der gleichartigen Wiederholung, da damit gefordert wird, den Prozess in verschiedenen Situationen unterschiedlich durchzuführen. Trotzdem macht es Sinn, sich im Rahmen der Planung von Kommunikationsprozessen dieser Anforderung zu stellen. In der zwischenmenschlichen Kommunikation sind wir es nämlich durchaus gewohnt, unsere Kommunikation flexibel auf verschiedene Situationen anzupassen. Wenn wir z. B. einen Freund darum bitten, uns bei dem Aufbau eines Gartenhäuschens zu helfen, werden wir ihm vielleicht eine E-Mail schicken, um zu fragen, ob er am nächsten Wochenende Zeit hat. Wenn wir dieselbe Bitte anbringen wollen, die Hilfe aber sofort benötigen, weil wir z. B. schon angefangen haben, das Gartenhäuschen aufzubauen und jetzt merken, dass wir eine helfende Hand benötigen, werden wir ihn wohl eher anrufen, um zu fragen, ob er Zeit hat.

Um also dieselbe Art von Kommunikation durchzuführen (in diesem Fall „um Hilfe bitten“) wählen wir je nach Situation unterschiedliche Wege. In der Unternehmenskommunikation könnte man vielleicht überlegen, dass wir es dann ja mit unterschiedlichen Kommunikationsprozessen zu tun haben, einmal einen Prozess für die zeitunkritischen Anfragen und einen Prozess für die zeitkritische Anfrage. Da wir ähnliche Effekte aber in sehr vielen Kommunikationsprozessen haben, kann das sehr leicht zu einer unübersichtlichen Prozesslandschaft führen, in der sich unsere Anwender dann nicht mehr zurechtfinden.

Es macht daher meines Erachtens mehr Sinn, für eine Art von Kommunikation, definiert durch das zu erreichende Ergebnis, auch einen Prozess vorzusehen, diesen dann aber so zu gestalten, dass er für unterschiedliche Rahmenbedingungen auch unterschiedliche Ausführungsoptionen erlaubt. Beispielsweise können wir für zeitkritische Berichte ein Attribut in der Eingabe vorsehen (etwa in Form einer Checkbox), mit dem wir dem Empfänger zeigen, dass wir eine schnelle Reaktion fordern. Am anderen Ende des Prozesses kann dieses Attribut wiederum für eine schnelle Benachrichtigung sorgen.

Wir alle kennen entsprechende Verfahren schon aus der E-Mail-Kommunikation. Im SMTP-Protokoll ist ein Flag (Nachrichtenattribut) vorgesehen, das eine Nachricht als dringend markiert bzw. mit hoher Priorität versieht. Diese Markierung wird dem Empfänger in seinem E-Mail-Programm in der Regel auch angezeigt und er kann entsprechend reagieren. Da damit eine schnelle Reaktion angefordert wird, macht es im Übrigen wenig Sinn, die Markierung in seinem E-Mail-Programm als Standard zu setzen. Wenn jede Nachricht markiert wird, ist schließlich keine mehr dringend, da es keinen Unterschied zum Normalfall mehr gibt. Damit wird auch deutlich, dass solch einfache Markierungen immer auch einer unterstützenden Vereinbarung bedürfen. Es muss den Kommunikationspartnern klar sein, was es heißt, wenn eine entsprechende Option gesetzt wird: „Was teile ich dem Empfänger damit mit?“ und „Was wird von mir als Empfänger damit erwartet?“.

Auf Basis dieses allgemeinen Überblicks über die funktionalen und nicht-funktionalen Anforderungen unserer Kommunikationsprozesse erkennen wir recht schnell, dass wir diese nicht mit einem einfachen Werkzeug erfüllen werden können, sondern dass dafür eine ganze Reihe von Werkzeugen nötig sind. Microsoft ist einer der Anbieter, die uns dabei auf jeder Ebene unterstützen können. Werfen wir daher im Folgenden einen Blick auf die Plattformkomponenten von Microsoft, mit denen wir die Anforderungen umsetzen werden.

3 Kommunikations-unterstützende Plattformen von Microsoft

Möchten wir die im vorigen Kapitel beschriebenen funktionalen und nicht-funktionalen Anforderungen der zu planenden Kommunikationsprozesse mithilfe einer IT-Infrastruktur umsetzen, benötigen wir dafür eine ganze Reihe von Diensten und Anwendungen. Microsoft hat im Laufe der Jahre seine Infrastrukturkomponenten soweit entwickelt, dass sie beinahe alle Anforderungen nativ erfüllen können. Natürlich bieten auch andere Anbieter entsprechende Komponenten. Zu nennen sind hier insbesondere IBM mit seiner Tochter Lotus und den Produkten Notes/Domino oder auch Oracle mit seiner Communications Suite. Nach meiner Erfahrung erreichen sie aber nicht den Integrationsgrad, der die Microsoft-Anwendungen auszeichnet. Dabei macht sich die inzwischen sehr starke Basis von Microsoft bei den Server- und Client-Betriebssystemen ebenso bezahlt wie die weite Verbreitung von Microsoft Office als einheitliche Büroanwendung in Unternehmen.

Im Folgenden möchte ich einen Überblick über die benötigten Dienste und Produkte geben und dabei deutlich machen, welche Anforderungsklasse wir mit welchem der Produkte abdecken können. Wir beschränken uns dabei in zweierlei Hinsicht. Einerseits betrachten wir nur Produkte, die wir unter dem Begriff Plattform beschreiben können, das heißt wir lassen Spezialanwendungen wie Team Foundation Server, Navision und Dynamics oder auch Project Server außer Betracht und beschränken uns auf frei konfigurierbare Plattformen, die uns den größtmöglichen Grad an Flexibilität erlauben. Das heißt nicht, dass es nicht sinnvoll sein kann, die oben genannten Spezialanwendungen einzusetzen, um damit bestimmte Anforderungen abzudecken. Diese Produkte sind aber immer schon für konkrete Einsatzbereiche wie zum Beispiel Softwareentwicklung (Team Foundation Server), Buchhaltung und Finanzen (Navision) und Projekt- und Portfoliomanagement (Project Server) entwickelt und spielen ihre Vorteile auch nur in diesen Einsatzbereichen aus. Uns geht es hier um Kommunikation im Unternehmen aus einer allgemeinen Perspektive. Daher werden wir diese Spezialfälle nicht betrachten.

Die zweite Einschränkung, die wir vornehmen, besteht darin, dass wir keine proprietären Anwendungen auf den noch zu beschreibenden Plattformen einsetzen werden, weder von uns noch von Drittanbietern. Wir beschränken uns rein auf die Standardfunktionen und –Konfigurationen, die die Plattformen ab Werk zur Verfügung stellen. Alle in Kapitel 2 beschriebenen Anforderungen lassen sich durch bewusste Integration der Plattformen abdecken. Wir werden nichts wirklich programmieren, einzig an einigen Stellen werden wir einfache Codeanpassungen vornehmen und VBA-Skripte verwenden müssen. Die technisch weitreichendsten Eingriffe werden SharePoint Designer-Workflows sein, die wir aber rein

über die grafische Oberfläche des SharePoint-Designers erstellen werden. Wo detaillierte Programmierung sinnvoll sein könnte, werden wir in der Umsetzung aber darauf hinweisen.

3.1 Active Directory

Basis einer jeden Microsoft-Infrastruktur ist ein gut designtes und gepflegtes Active Directory. Active Directory ist der von Microsoft mit Windows 2000 eingeführte Verzeichnisdienst zur Verwaltung der IT-Infrastruktur eines Unternehmens. Seine Hauptaufgaben bestehen in der Authentifizierung der Benutzer, der Verwaltung von Geräten und Benutzern, der zentralen Speicherung von Konfigurationsdaten und der Steuerung der Rechte innerhalb der Infrastruktur. Er basiert auf drei Industriestandards, dem Domain Naming System (DNS), dem Lightwight Directory Access Protocol (LDAP) und dem Authentifizierungsverfahren Kerberos Version 5.

Die Daten des Active Directory werden in einer verteilten, relationalen Datenbank gespeichert. Die Inhalte der Datenbank werden auf die zentralen Verwaltungsserver, die sogenannten Domänencontroller repliziert. Verschiedene Inhalte werden in unterschiedlichen Datenbankbereichen, sogenannten Partitionen gespeichert. Jede Partition hat ihren eigenen Replikationsbereich. Die wichtigsten Partitionen sind die Schemapartition, die Konfigurationspartition und die Domänenpartition(en). Darüber hinaus werden weitere Anwendungspartitionen, wie zum Beispiel für die DNS-Daten, eingesetzt.

Die Schemapartition enthält das Datenbankschema. Darüber ist definiert, welche Objekte mit welchen Eigenschaften in der Datenbank angelegt werden können. Anwendungen, die eigene Objekte oder Attribute in der Datenbank benötigen, müssen daher das Schema anpassen. Bekanntestes Beispiel ist hier Microsoft Exchange. Da Exchange Informationen an Benutzerobjekten speichert, wie zum Beispiel Informationen zum Postfach, müssen entsprechende Attribute im Datenbankschema angelegt und mit Benutzerobjekten verbunden werden.

In der Konfigurationspartition liegen Informationen zur Konfiguration des Verzeichnisdienstes, zum Beispiel welche Dienste eingerichtet sind und auf welchen Servern bereitgestellt werden. Hier speichert Exchange Informationen über seine Serverstruktur. Andere zentrale Serverdienste werden in der Konfigurationspartition über Zugriffspunkte (Service Connection Point, SCPs) abgebildet. Weitere Informationen, die in der Konfigurationspartition gespeichert werden, sind zum Beispiel die Domänenstruktur des Active Directory und die Vertrauensstellungen.

In der Domänenpartition schließlich liegen die Informationen über alle Objekte in der Domäne. Hier finden wir insbesondere alle Konten, Benutzer, Computer und Gruppen, die sich in der Domäne authentifizieren können und denen Rechte vergeben werden können. Diese Art von Objekte heißen Sicherheitsprinzipale. Da das Active Directory (AD) nicht nur aus einer, sondern aus einer hierarchisch gestaffelten Struktur von Domänen bestehen kann, kann das AD auch mehrere Domänenpartitionen enthalten. Für die Strukturierung verwendet das AD das System des DNS, also eine hierarchische Benennung, in der ganz rechts die oberste Ebene der Hierarchie benannt wird und ganz links der aktuelle Endknoten der Hier-

archie, also nach dem Muster *Server1.Unterdomäne1.Unternehmensdomäne.TopLevelDomäne* (zum Beispiel *SP01.Finance.Hauenherm.com*). Domänen stellen Sicherheitsgrenzen im AD dar. Konten liegen immer innerhalb einer Domäne und haben Rechte innerhalb dieser Domäne. Die Summe aller Domänen nennt Microsoft die Gesamtstruktur des Active Directory. Alle Domänen innerhalb der Gesamtstruktur verwenden dasselbe Datenbankschema und sind über Vertrauensstellungen verbunden, so dass Benutzer einer Domäne auch Rechte in einer anderen Domäne bekommen können und sichergestellt ist, dass alle Eigenschaften eines Objektes auch in allen anderen Domänen gelesen werden können.

Für die Binnenstrukturierung werden innerhalb der Domänen sogenannte Organisationseinheiten (Organizational Units, OUs) angelegt. Diese dienen dazu, Objekte nach bestimmten Kriterien zusammenzufassen, zum Beispiel alle Benutzer der Finanzabteilung oder alle Computer mit einem Standarddesktop. OUs haben keine Auswirkungen auf die Rechte der Benutzer und sind auch selbst keine Sicherheitsprinzipale. Sie können aber als Bereich für die Anwendung von Konfigurationseinstellungen über Gruppenrichtlinien verwendet werden. Gruppenrichtlinien dienen dazu, Konfigurationseinstellungen zentral zu steuern und auf mehrere Objekte anzuwenden. Gruppenrichtlinienobjekte können mit Domänen, Standorten und eben OUs verbunden werden, so dass die Einstellungen für alle Objekte innerhalb des verbundenen Bereichs angewendet werden. In einigen Fällen werden wir Gruppenrichtlinien nutzen, um Benutzern einheitliche Einstellungen zukommen zu lassen. Gruppenrichtlinien ermöglichen auch die zentrale Verteilung von Zertifikaten oder Richtlinien digitaler Rechte.

Objekte innerhalb einer Domäne werden im Active Directory standardmäßig über ihre LDAP-Namen angesprochen nach dem Muster *cn=Server1,ou=Organisationseinheit1,dc=Unterdomäne1,dc=Unternehmensdomäne,dc=TopLevelDomäne,* also zum Beispiel *cn=SPS01,ou=finance,dc=finance,dc=hauenherm,dc=com*. Wie DNS-Namen lesen sich auch diese Namen von rechts nach links, das heißt am Anfang des Namens (also links) steht das Objekt, das angesprochen wird (hier der Server SPS01) und der Rest des Namens spiegelt die hierarchische Einordnung im Verzeichnisbaum wider, wobei der oberste Domänenteil ganz rechts steht (vgl. Bild 3.1):

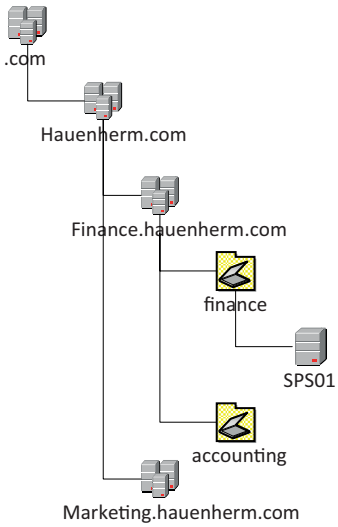

Bild 3.1
Active Directory-Struktur

Neben dieser logischen Strukturierung ermöglicht das AD auch noch eine davon unabhängige Strukturierung der Objekte nach Standorten. Diese werden durch die zugehörigen IP-Netze definiert und werden unter anderem dazu genutzt, Kommunikationswege und Replikationsverbindungen zu berechnen.

Da das Active Directory für alle Objekte Zugriffsteuerungslisten (Access Control Lists, ACLs) pflegt und innerhalb der hierarchischen Struktur sowohl die Vererbung von Berechtigungen erlaubt, als auch die Vergabe dedizierter Berechtigungen auf den einzelnen Ebenen, stehen viele Möglichkeiten zur Administration des Active Directorys zur Verfügung. Man kann stark zentralisiert arbeiten und die administrativen Aufgaben in einem kleinen Personenkreis der IT-Administratoren zusammenfassen oder ein dezentrales Verwaltungsmodell einrichten, bei dem ein Teil der administrativen Aufgaben an die Benutzer delegiert wird. Im letzten Fall reichen die delegierbaren Aufgaben von der Pflege der eigenen Kontoinformationen, die im AD gespeichert werden, wie zum Beispiel Abteilungszugehörigkeit, Telefonnummern und Standortinformationen, über die Benutzerverwaltung in der eigenen Abteilung, wie dem Anlegen neuer Benutzerkonten, bis hin zur Verwaltung eigener Benutzergruppen und Empfängerlisten.

Gerade die Möglichkeiten der Dezentralisierung werden im Rahmen der Umsetzung der Kommunikationsprozesse von Bedeutung sein. Damit wird die Grundlage dafür geschaffen, dass abteilungsinterne Kommunikationsprozesse vollständig von den betroffenen Benutzern umgesetzt werden. So kann zum Beispiel die Personalabteilung eine Formularbibliothek in SharePoint für den E-Mail-Empfang aktivieren und die Mailadresse im Adressbuch des Unternehmens veröffentlichen, indem ein entsprechender Kontakteintrag im Active Directory angelegt wird. Oder die Abteilung kann sich selbständig eine Empfängerliste erstellen und diese im AD veröffentlichen, so dass E-Mails an diese Adresse an alle Benutzer der Abteilung weitergeleitet werden.

Im Einzelfall steht dahinter natürlich immer eine strategische Entscheidung des Unternehmens darüber, wie viel Autonomie an die Benutzer übertragen werden soll. Je mehr die Benutzer ohne Inanspruchnahme der IT konfigurieren können, desto geringer wird die Steuerbarkeit dieser Konfigurationseingriffe. Hier ist eine Abwägung vorzunehmen. Einige der in diesem Buch später zu betrachtenden Kommunikationsverfahren können aber auch dafür genutzt werden, Änderungen nachzuvollziehen und sie damit besser steuerbar zu machen.

Bleibt noch die Frage, welche Objekte des Active Directorys für die Gestaltung unserer Kommunikationsprozesse wir kennen müssen. Dies sind insbesondere die zwei zentralen Sicherheitsprinzipale, Benutzerkonten und Gruppenkonten.

Benutzerkonten repräsentieren natürliche oder virtuelle Personen im Unternehmen. Jeder Mitarbeiter und jeder Dienst, der auf das AD zugreifen muss und über Zugriffsrechte gesteuert werden muss, benötigt ein Benutzerkonto. Es verwundert daher nicht, dass eben nicht nur Mitarbeiter, sondern auch Dienste und Geräte im AD über Benutzerkonten verfügen, über die wir steuern können, was diese innerhalb unserer Infrastruktur dürfen. Das Active Directory speichert aber nicht nur die reinen Authentifizierungsinformationen zu den Benutzern, sondern dient auch als Adressbuch des Unternehmens, in dem eine Reihe weiterer Informationen abgelegt werden können. Dies sind zum Beispiel Kontaktinformationen wie Adressen, Telefonnummern und Ähnliches, aber auch organisatorische Informationen wie die Abteilungszugehörigkeit, der direkte Vorgesetzte oder Gruppenmitglied-

schaften. All diese Informationen eines Benutzerkontos sind abfragbar und können von uns in unseren Kommunikationsprozessen genutzt werden. Darüber hinaus lässt sich das Active Directory um eigene Attribute erweitern.

Sind Informationen dieser Art im AD zu speichern, ohne dass sie mit einem Benutzerkonto verbunden werden sollen, kann der spezielle Objekttyp *Kontakt* genutzt werden. An diese Objekte können Adressinformationen für eine Person hinterlegt werden. Da es sich bei einem Kontakt aber nicht um einen Sicherheitsprinzipal handelt (Kontakte bekommen keine SID, Security Identifier), können diesen keine Rechte gegeben werden. Für die externe Kommunikation im Unternehmen können sie aber durchaus relevant sein, da Kontakte zum Beispiel auch als Empfänger in Empfängerlisten genutzt werden können. In SharePoint werden Kontakte zum Beispiel genutzt, um die Mailadressen E-Mail-aktivierter Bibliotheken zu veröffentlichen. Auch Exchange greift auf diese Objekte zu, um externe Mail-Adressen im Adressbuch zu veröffentlichen.

Gruppenkonten dienen im Active Directory insbesondere dazu, die Berechtigungsverwaltung zu vereinfachen und übersichtlich zu gestalten. Eine Benutzergruppe kann eine SID (einen Security Identifier) bekommen, das heißt ein Sicherheitsprinzipal sein, dem Berechtigungen vergeben werden können. Diese Berechtigungen vererben sich an alle Benutzer dieser Gruppen. Hat eine Gruppe einen Sicherheitsprinzipal, wird sie im AD als Sicherheitsgruppe bezeichnet, im Unterschied zu den Verteilergruppen, die keine SID haben und denen daher auch keine Berechtigungen vergeben werden können.

Die Planung der Gruppen ist ein eigenes Kapitel des Active-Directory-Designs und kann in großen Umgebungen sehr aufwendig sein. Gruppen verfügen über unterschiedliche Einsatzbereiche, die festlegen, wo einer Gruppe Rechte gegeben werden können und aus welchen Bereichen die Mitglieder kommen können. Es werden lokale, domänenlokale, globale und universelle Gruppen unterschieden, abhängig davon, ob der Gruppe nur in der eigenen Domäne oder auch in der Gesamtstruktur Rechte gegeben werden können, und ob die Gruppe nur Benutzer aus der eigenen Domäne oder auch aus anderen vertrauten Domänen beziehungsweise anderen Domänen der Gesamtstruktur enthalten kann. Darüber hinaus können Gruppen nahezu beliebig ineinander geschachtelt werden. Außerdem kann ein Benutzer Mitglied mehrerer Gruppen sein, wobei sich die einzelnen Gruppenberechtigungen wieder gegenseitig aushebeln können. Da dies kein Buch über das Active Directory selbst werden soll, werde ich diese Aspekte hier nicht genauer erläutern, sondern bei Bedarf auf die notwendigen Einstellungen hinweisen.

Eine Anwendung, die sehr intensiv mit den im Active Directory angelegten Gruppen arbeitet beziehungsweise auch selbst Gruppen im Active Directory anlegt, ist Microsoft Exchange. Alle Arten von Berechtigungen in Exchange und alle Empfänger- und Verteilerlisten basieren auf entsprechenden Active Directory-Gruppen. Dabei sei schon vorweggenommen, dass Exchange sogenannte universelle Gruppen (ein spezieller Typ der Active Directory-Gruppen) benötigt, da diese Listen in der gesamten Domänenstruktur des Unternehmens verwendbar sein müssen und Konten aus allen Domänen der Gesamtstruktur enthalten können.

Im Gegensatz dazu erlaubt SharePoint zwar die Verwendung von Active Directory-Gruppen, bietet aber auch ein eigenes Gruppenkonzept an, das es ermöglicht, unabhängig von der AD-Struktur Berechtigungen zu verwalten.

3.1.1 Active Directory Certificate Services

Die Nutzung digitaler Zertifikate gehört heute in den meisten IT-Umgebungen zum Standard. Gerade die Server-zu-Server-Kommunikation wird inzwischen standardmäßig mit zertifikatsbasierten Authentifizierungs- und Verschlüsselungsmechanismen durchgeführt. Auch in der im folgenden beschriebenen Microsoft-Umgebung ist das feststellbar. Exchange Server und Skype for Business verwenden standardmäßig Zertifikate für die Kommunikation mit ihren Clients. Dafür werden nach der Installation dieser Anwendungen selbstsignierte Zertifikate erstellt. Diese haben den Nachteil, dass sie in keine Zertifizierungsstellenhierarchie eingebunden sind und die Vertrauenswürdigkeit nur durch explizites Akzeptieren der Zertifikate hergestellt wird. Schon aus diesem Grund ist es sinnvoll, über die Einrichtung einer eigenen Zertifizierungsstelle im Unternehmen nachzudenken. Eine interne Zertifizierungsstelle stellt eine vertrauenswürdige Quelle aller verwendeten Zertifikate sicher. Die von dieser Zertifizierungsstelle ausgestellten Zertifikate kann für viele weitere Anwendungen genutzt werden. So können zum Bespiel Zertifikate für die Signatur und Verschlüsselung von E-Mails und Daten genutzt werden, für die Einrichtung von VPNs, für die Codesignatur eigener Skripte, für die Verschlüsselung des Datenverkehrs mittels IPSEC, für die Überwachung des Zustandes unseres Clients mit Network Access Protection, für den Aufbau sicherer Websites mittels HTTPS und noch vieles mehr.

Machen wir uns zuerst mit der Funktionsweise von Zertifikaten in einer Public-Key-Infrastruktur (PKI) vertraut. Zertifikate bestehen in der Regel aus zwei Teilen, einem öffentlichen und einem privaten Schlüssel. Die Erzeugung dieser Schlüssel basiert auf einer Zertifikatsanforderung, bei der sich der Benutzer (oder die Maschine) in irgendeiner Form ausweisen muss. Man unterscheidet verschiedene Klassen von Zertifikaten auf Basis der Art, wie Benutzer sich ausweisen. Bei starken Personenzertifikaten muss der Antragsteller persönlich bei der Zertifizierungsstelle vorstellig werden und sich mit einem gültigen Ausweispapier ausweisen. Die Zertifizierungsstelle garantiert damit, dass das Schlüsselpaar tatsächlich für diese Person ausgestellt wurde.

Wie die Namen schon vermuten lassen, bleibt der private Schlüssel im alleinigen Besitz des Inhabers und kann nur von diesem genutzt werden. Der öffentliche Schlüssel hingegen wird veröffentlicht und kann von allen Benutzern, die Zugriff auf den öffentlichen Schlüsselspeicher haben, eingesetzt werden. Der private Schlüssel dient in erster Linie dazu, den Besitzer auszuweisen, indem der Benutzer die von ihm gesendeten Daten mit dem privaten Schlüssel signiert. Dabei wird mithilfe des Schlüsselalgorithmus ein Hash über die Daten berechnet. Dieser Hash wird sofort ungültig, wenn die Daten verändert werden. Der Hashwert wiederum wird mit dem privaten Schlüssel verschlüsselt und kann nur mit dem öffentlichen Schlüssel entschlüsselt werden. Damit ist zweierlei sichergestellt, erstens dass die Daten tatsächlich vom ausgewiesenen Absender kommen und zweitens, dass sie nach der Signierung nicht mehr verändert wurden.

Der öffentliche Schlüssel dient vor allem dazu, sicherzustellen, dass der Inhalt nur vom beabsichtigten Empfänger gelesen werden kann, also zur Verschlüsselung von Daten. Dabei werden die Daten mit dem öffentlichen Schlüssel verschlüsselt, so dass sie nur der Besitzer des dazugehörigen privaten Schlüssels entschlüsseln kann.

Die Schlüssel sind also aufeinander bezogen, das heißt, was mit dem privaten Schlüssel signiert wurde, kann mit dem öffentlichen Schlüssel geprüft werden. Dadurch ist sicherge-

stellt, dass die Daten tatsächlich vom ausgewiesenen Absender kommen. Was mit dem öffentlichen Schlüssel verschlüsselt wurde, kann nur mit dem dazugehörigen privaten Schlüssel entschlüsselt werden. In einigen Anwendungsfällen werden für die Verschlüsselung auch noch weitere Mechanismen eingesetzt, zum Beispiel Kombinationen aus symmetrischen und den hier beschriebenen asymmetrischen Verschlüsselungsverfahren (wie zum Beispiel im Encrypting File System (EFS) von Windows-Betriebssystemen). Diese grundlegende Darstellung soll aber für unsere Zwecke reichen.

Die Arbeit mit Zertifikaten ist nur dann sinnvoll, wenn damit auch wirklich sichergestellt ist, dass der im Zertifikat ausgewiesene Besitzer auch tatsächlich der Inhaber des Zertifikates ist. Sinn dabei ist es gerade, den Besitzer auszuweisen, ohne dass er persönlich erscheinen muss. Dafür müssen verschiedene Anforderungen erfüllt sein:

1. Dem Aussteller des Zertifikates muss dahingehend vertraut werden, dass er eine ausreichende Identitätsprüfung bei der Ausstellung des Zertifikates vorgenommen hat.
2. Das Zertifikat muss regelmäßig überprüft bzw. erneuert werden, das heißt es darf auch nur im Zeitraum seiner Gültigkeit verwendet werden.
3. Das Zertifikat darf nicht inzwischen widerrufen worden sein, weil zum Beispiel der private Schlüssel in falschen Besitz gelangt ist.
4. Derjenige, der das Zertifikat vorweist beziehungsweise als Absender benannt ist, muss derjenige sein, der auf dem Zertifikat benannt wird.
5. Der tatsächliche Einsatz des Zertifikats muss mit einem der im Zertifikat benannten Einsatzzwecke übereinstimmen.

Genau diese Überprüfungen finden in zertifikatsbasierter Kommunikation statt. Wenn Sie zum Beispiel über HTTPS auf eine Website zugreifen, weist die Website sich mit einem Serverzertifikat aus. Dieses Zertifikat überprüft Ihr Browser folgendermaßen:

- Lautet der Name auf dem Zertifikat so wie die Website, die aufgerufen wurde?
- Ist das Zertifikat schon und noch gültig?
- Kann ich überprüfen, ob es widerrufen wurde?
- Handelt es sich um ein Zertifikat zur Identifikation eines Webservers?
- Stammt es von einer vertrauenswürdigen Zertifizierungsstelle?

Schlägt eine dieser Prüfungen fehl, erhalten Sie in der Regel eine Zertifikatswarnung in Ihrem Browser, mit einem Hinweis, welche der Prüfungen gescheitert ist.

Grundsätzlich bestehen zwei Möglichkeiten, im Unternehmen Zertifikate einzusetzen. Erstens, Sie kaufen die benötigten Zertifikate von einer öffentlichen Zertifizierungsstelle. Das hat den Vorteil, dass die Zertifikate von Beginn an vertrauenswürdig sind und keine weiteren Konfigurationen erforderlich ist. Nachteile dieses Verfahrens sind, dass es bei einer großen Menge von Zertifikaten sehr aufwendig sein kann, die unterschiedlichen Laufzeiten im Blick zu behalten und die Erneuerung der Zertifikate vorzunehmen. Je nach Menge und Art der benötigten Zertifikate kommen in diesem Fall zudem eventuell hohe Kosten zusammen.

Die zweite Möglichkeit besteht im Aufbau einer eigenen, unternehmensinternen Zertifizierungsstelle. Der Nachteil ist in diesem Fall, dass die Zertifikate einer internen Zertifizierungsstelle auf externen Clients nicht ohne Weiteres als vertrauenswürdig sind. Außerdem

sind die Zertifizierungsstelle und die Ausstellung der Zertifikate selbst zu administrieren. Vorteil ist aber, dass die Kosten bei einer großen Menge benötigter Zertifikate sehr überschaubar sind, da dazu keine eigenen Lizenzen für die Zertifizierungsstelle erforderlich sind. Die Active Directory Certificate Services sind Bestandteil der Windows Server-Lizenz.

In größeren Umgebungen empfiehlt sich ein mindestens dreistufiger Aufbau einer Zertifizierungsstellenhierarchie, bestehend aus einer Offline-Root-Zertifizierungsstelle, einer oder mehreren Richtlinien-Zertifizierungsstellen und mehreren ausstellenden Zertifizierungsstellen. Nur die Zertifizierungsstellen der untersten Ebene stellen Zertifikate für Benutzer und Computer aus. Die Root-Zertifizierungsstelle stellt nur die Zertifikate für die Richtlinien-Zertifizierungsstellen aus und diese wiederum die Zertifikate für die ausstellenden Zertifizierungsstellen. Auf der Ebene der Richtlinien-Zertifizierungsstellen werden die Ausstellungsrichtlinien für die Zertifikate verwaltet und veröffentlicht (vgl. Bild 3.2).

In kleineren Umgebungen wird die Struktur häufig auf zwei Ebenen reduziert, der Offline-Root-Zertifizierungsstelle und einer oder mehrerer AD-integrierter ausstellender Zertifizierungsstellen.

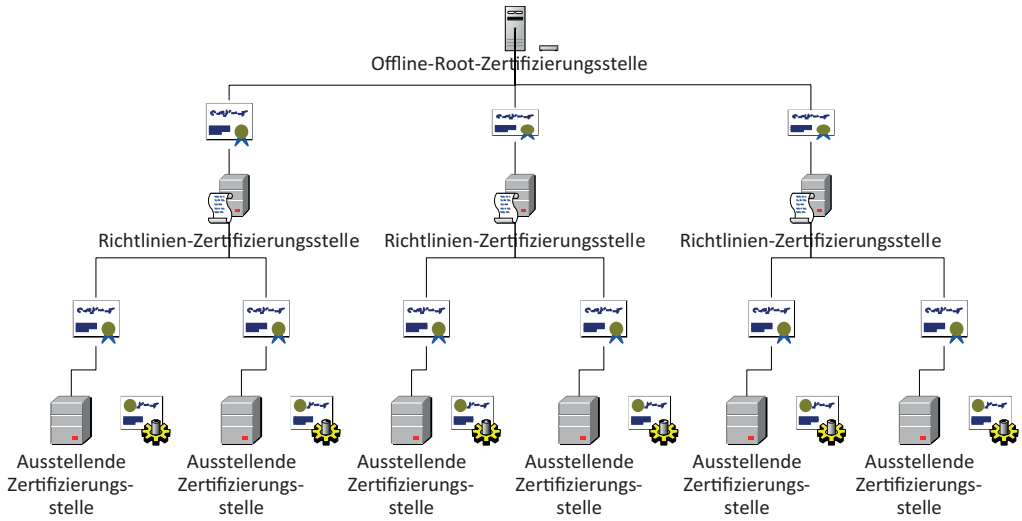

Bild 3.2 Typischer Aufbau einer Zertifizierungsstellenhierarchie

Auf eine Offline-Root-Zertifizierungsstelle sollte auch in kleinen Umgebungen nicht verzichtet werden. Diese Zertifizierungsstelle wird genutzt, um das erste Zertifikat der Hierarchie auszustellen und die Zertifikate der davon abgeleiteten Zertifizierungsstellen. Sie kann gut als virtuelle Maschine auf einer externen Festplatte oder einem anderen Datenträger gespeichert werden und muss nur zur Erneuerung der Zertifikate und zur Veröffentlichung der Sperrlisten online genommen werden. Dadurch wird die Gefahr einer Korrumpierung dieser Zertifizierungsstellen weitestgehend ausgeschlossen. Wenn aus irgendeinem Grund die Zertifikate einer der ausstellenden Zertifizierungsstellen korrumpiert sein sollten, können diese Zertifizierungsstellen einfach neu erstellt werden, ohne dass die gesamte Vertrauenshierarchie erneuert werden muss. Das heißt, alle Clients, die den alten Zertifizierungsstellen vertraut haben, vertrauen automatisch auch den neuen, da sie ja wieder zur selben Quelle zurückverfolgt werden können.

Die Active Directory Certificate Services im Windows Server unterstützen zwei grundlegende Einrichtungsarten für Zertifizierungsstellen, eigenständige und unternehmensinterne Zertifizierungsstellen. Erstere werden unabhängig vom Active Directory aufgebaut und unterstützen keine Zertifikatsvorlagen, letztere werden in das AD integriert – das heißt, das Zertifizierungsstellenzertifikat wird im AD veröffentlicht und von allen AD-Clients automatisch als vertrauenswürdig anerkannt. Die Root-Zertifizierungsstelle sollte als eigenständige Zertifizierungsstelle eingerichtet werden – aus dem oben genannten Grund der Absicherung gegen eine Korrumpierung des Root-Zertifikats. Selbst wenn das gesamte Active Directory des Unternehmens neu aufgebaut werden muss, bleibt die Quelle der Vertrauenswürdigkeit bestehen, da das Rootzertifikat identisch bleibt. Dabei sind aber einige Punkte zu beachten. Das Rootzertifikat wird nicht automatisch an alle Clients veröffentlicht. Dies muss manuell eingerichtet werden. Dazu wird das Rootzertifikat im Konfigurationsspeicher des Active Directory als vertrauenswürdige Root-Zertifizierungsstelle eingebunden. Außerdem müssen die AIA- (Authority Information Access) und CDP-Pfade (Certificate Revocation List Distribution Point) angepasst werden. Dies geschieht in den Einstellungen der Zertifizierungsstellen. Da die Pfade in den von der Zertifizierungsstelle ausgestellten Zertifikaten benannt und von den Clients zur Überprüfung genutzt werden, sollte sichergestellt sein, dass die hier benannten Pfade für alle Clients erreichbar sind. Wenn die Zertifikate also auch von externen Clients überprüft werden müssen, sollte mindestens einer der Pfade auf einen öffentlich erreichbaren Server verweisen, am besten auf ein Verzeichnis auf einem Webserver. Dazu kann der Pfad als URL angegeben werden. Weitere mögliche Verweistypen sind UNC- und LDAP-Pfade.

Diese Hinweise sollen genügen, um die wichtigsten Anforderungen an die Einrichtung der Zertifizierungsstellen zusammenzufassen. Fundierte Anleitungen zum Aufbau und zur Konfiguration einer Zertifizierungsstellenhierarchie finden sich in der TechNet-Library (*https://technet.microsoft.com/de-DE/library/hh831348.aspx*) und der einschlägigen Windows Server-Literatur.

Wofür wir die Zertifikatsdienste bei der Gestaltung unserer Kommunikationsprozesse benötigten, sollte aus der vorangegangenen Beschreibung deutlich geworden sein. Immer dort, wo Verschlüsselung und Nachvollziehbarkeit zentrale Anforderungen darstellen, können diese mithilfe von Zertifikaten umgesetzt werden. Außerdem werden wir Zertifikate auch als integrierten Bestandteil anderer Dienste, wie den im Folgenden beschriebenen Active Directory Rights Management Services wiederfinden.

3.1.2 Active Directory Rights Management Services

Mit der immer weiter fortschreitenden Digitalisierung von Informationen und der damit einhergehenden erleichterten Weitergabe und Weiterverarbeitung der Informationen entstehen auch für Unternehmen neue Herausforderungen. Viele Beispiele in jüngster Zeit zeigen, wie leicht Informationen in unberechtigte Hände gelangen können und anschließend gegen die Interessen des rechtmäßigen Besitzers verwendet werden können. Diese Diskussion betrifft nicht nur die klassischen Branchen, in denen Informationen gehandelt werden, wie zum Beispiel Verlage und die Musikindustrie, sondern auch alle anderen Unternehmen, in denen vertrauliche Informationen anfallen. Denken Sie nur an die Pro-

duktentwicklung oder die Personaldaten in einem Unternehmen. Solange diese Daten nur auf Papier vorlagen, konnten sie relativ einfach vor unberechtigter Verwendung geschützt werden, indem Schränke und Räume abgeschlossen wurden. In dem Moment, wo Daten digital gespeichert und über teilweise öffentliche Netzwerkverbindungen transportiert werden, ist der Schutz nicht mehr so leicht möglich. Natürlich kann der Transportweg abgesichert werden, zum Beispiel über verschlüsselte Verbindungen oder auch durch Schützen der Speicherorte gegen unberechtigten Zugriff über Zugriffsrechte. Wird das Dokument aber erst einmal an einen anderen Ort verschoben, der nicht vom Unternehmen verwaltet wird, sind diese Schutzmechanismen ausgehebelt. Verschicken wir die Konstruktionszeichnungen an einen unserer Lieferanten, sind wir darauf angewiesen, dass dieser die Daten genauso schützt, wie wir es tun. Geschieht das nicht, haben wir ein Datenleck, das unserem Unternehmen schaden kann.

Um den Schutz der Informationen auch sicherzustellen, wenn diese das Unternehmen verlassen, kann die Verwaltung digitaler Rechte helfen. Hierunter versteht man ein an das Dokument selbst gebundenes Rechtemanagement. Das heißt, das Dokument „weiß“, wer was mit ihm machen darf, wer es bearbeiten darf, wer es ausdrucken darf, wer es weiterleiten darf usw. und verhindert unberechtigte Aktionen. Wichtig ist, dass diese Rechte nicht wie klassische Zugriffsrechte über den Speicherort verwaltet werden und außer Kraft gesetzt sind, wenn das Dokument an einen anderen Ort bewegt wird, sondern am Dokument erhalten bleiben, wo immer es sich auch befindet.

Eine solche Funktion erfordert natürlich zweierlei, erstens Dokumente, die entsprechende Rechte speichern können, und zweitens Anwendungen, die diese Rechte lesen und anwenden können. Außerdem natürlich einen Mechanismus zur Vergabe dieser Rechte. In unserer Microsoft-Umgebung finden wir alles dafür vorbereitet. Office-Dokumente sind spätestens seit der Version 2010 in der Lage, digitale Rechte zu tragen, alle Anwendungen der Office-Palette, wie Word, Excel und PowerPoint, aber auch Outlook und Exchange, genauso wie SharePoint können mit diesen Rechten umgehen. Die Vergabe der Rechte erfolgt über die Anbindung an die Active Directory Rights Management Services (ADRMS).

Die Anwendung digitaler Rechte erfolgt über Richtlinien, in denen Aktionen definiert werden, die die Empfänger der Dokumente an diesen durchführen dürfen, zum Beispiel das Drucken oder das Weiterleiten des Dokumentes. Die Richtlinien werden über den ADRMS-Server zentral definiert und können mithilfe von Gruppenrichtlinien auf die Clients der Anwender verteilt werden. In den kompatiblen Anwendungen können diese Richtlinien vom Autor oder Bearbeiter auf die Dokumente angewendet werden. Bei der Zuweisung einer Richtlinie zu einem Dokument wird dieses mithilfe eines speziellen Zertifikats verschlüsselt, einem sogenannte Client Licensor Certificate (CLC), und mit einer Veröffentlichungslizenz (Publishing License, PL) versehen. Will ein Benutzer auf ein derart verschlüsseltes Dokument zugreifen, erwirbt er über den Rechteverwaltungsserver eine Endbenutzerlizenz. Dabei überprüft der Server die Authentizität des Benutzers und bestimmt, ob dieser berechtigt ist, die entsprechende Lizenz zu erwerben. Hat der Benutzer die Lizenz erworben, kann er das Dokument öffnen und die laut Lizenz zugelassenen Aktionen am Dokument durchführen.

Innerhalb der Organisation mit einer einheitlichen AD-Gesamtstruktur erfolgt die Benutzerauthentifizierung über das Active Directory. Sollen die Rechte auch unternehmensübergreifend angewendet werden, können dafür entweder eigene Verfahren des ADRMS-Dienstes

angewendet werden oder auf die weiterreichenden Funktionen der Active Directory Federation Services zurückgegriffen werden. Im ersten Fall können im ADRMS-Dienst vertraute Benutzerdomänen (Trusted User Domains, TUDs) über Zertifikate eingerichtet werden. Diese ermöglichen es externen Benutzern, Endbenutzerlizenzen über den Rechteverwaltungsdienst des Unternehmens zu erwerben. Einen anderen Weg stellen vertraute Veröffentlichungsdomänen (Trusted Publishing Domains, TPDs) dar, bei denen die Benutzer über einen eigenen RMS-Dienst Lizenzen zum Entschlüsseln von Dokumenten beziehen, die vom RMS-Server eines anderen, vertrauten Unternehmens verschlüsselt wurden.

Voraussetzung für Active Directory Rights Management Services sind neben einem Active Directory und einem Serverzertifikat von einer vertrauenswürdigen Zertifizierungsstelle auch ein SQL Server, in dem die Konfigurationsdatenbank des Dienstes gespeichert wird. Da der Dienst als Webservice arbeitet, setzt er auch eine Installation der Internet Information Services (IIS) auf dem Verwaltungsserver voraus. Mit der aktuellen Version des Dienstes ist auch eine Erweiterung für mobile Geräte, wie zum Beispiel Smartphones, verfügbar. Damit können die Rechte auch beim Öffnen und Erstellen der Dokumente auf einem solchen Gerät angewendet werden.

Auch hier möchte ich mich auf diese Beschreibung beschränken. Einen vollständigen Überblick und weitere Informationen für die Einrichtung und Konfiguration des Dienstes ist wieder über TechNet verfügbar (*https://technet.microsoft.com/de-de/library/how-adrms-works.aspx*).

Wie uns dieser Dienst bei der Gestaltung unserer Kommunikationsprozesse unterstützen kann, sollte aus diesen Erläuterungen ersichtlich sein. Er stellt ein mächtiges Werkzeug zur Sicherstellung von Compliance-Anforderungen in der Kommunikation dar und ermöglicht eine detaillierte und granulare Steuerung der Weiterverarbeitung von Informationen und Dokumenten.

3.1.3 Active Directory Federation Services

Solange Kommunikationsprozesse rein unternehmensintern betrachtet und geplant werden, bietet das Active Directory alle erforderlichen Funktionen, um eine sichere und steuerbare Kommunikation zu ermöglichen. Selbst einzelne externe Kommunikationsprozesse lassen sich durch einfache Mechanismen authentifiziert abwickeln, zum Beispiel durch die Vergabe von Benutzerkonten an externe Benutzer. Komplizierter wird die Lage, wenn in den externen Kommunikationsprozessen eine Identifikation der externen Kommunikationspartner erfolgen muss, wir diese Personen aber nicht vorher benennen können. Wenn zum Beispiel unterschiedliche Mitarbeiter eines Partnerunternehmens auf interne Informationen zugreifen müssen, diese über ihre Rollen bestimmte Zugriffsrechte bekommen müssen, gleichzeitig aber sichergestellt sein muss, dass die Aktionen personenbezogen nachvollziehbar sind.

Setzt das Partnerunternehmen ebenfalls ein Active Directory ein, ließen sich zumindest die Authentifizierung und die Rechtevergabe auch über Gesamtstrukturvertrauensstellungen oder externe Vertrauensstellungen abwickeln. In diesem Fall wird die AD-Gesamtstruktur oder eine einzelne Domäne des Partnerunternehmens als vertrauenswürdig eingestuft. Damit wird erlaubt, dass den Benutzerkonten dieser Gesamtstruktur oder Domäne Rechte

in der vertrauenden Gesamtstruktur vergeben werden können. Wohlgemerkt wird damit nicht automatisch ein Zugriff gestattet, sondern nur die Möglichkeit geschaffen, Benutzerkonten, die sich nicht gegen das vertrauende AD authentifizieren, Zugriff zu geben. Kommen allerdings andere Authentifizierungsanbieter ins Spiel, wird die Sache deutlich komplexer. Hier können uns die Active-Directory-Verbunddienste oder die Active Directory Federation Services (ADFS) helfen.

Ziel der ADFS ist es, externen Benutzern ein Single Sign On (SSO), also die Authentifizierung und Autorisierung an verschiedenen Ressourcen mittels einer einmaligen Anmeldung zu ermöglichen. Dafür bietet ADFS zwei Mechanismen, einmal den sogenannten Geräteregistrierungsdienst, zum anderen die Einrichtung einer anspruchsbasierten Authentifizierung (Claim Based Authentication).

Die Geräteregistrierung erlaubt authentifizierten Benutzern, ihrem Benutzerkonto Computer hinzuzufügen, die selbst über kein Konto im Active Directory verfügen, wie zum Beispiel iOS-Geräte oder Windows-Geräte ohne Computerkonto im AD. Auch wenn das für die interne Kommunikation hilfreich ist, spielt dieses Verfahren für die Planung unserer Kommunikationsprozesse keine Rolle.

Zentraler ist der zweite Anwendungsbereich, die anspruchsbasierte Authentifizierung. Bei diesem Authentifizierungsverfahren liefert der zugreifende Benutzer in der Anmeldung Informationen über sich mit, anhand derer der ADFS-Dienst entscheidet, ob ein Benutzer Zugriffsrechte auf eine Ressource erhält oder nicht. Typische Arten von Informationen, sogenannten Ansprüchen, die dabei überprüft werden, sind Gruppenzugehörigkeiten, Name, Rolle, Benutzer-ID, E-Mail-Adresse, Standort, Zeitinformationen, Zertifikatseigenschaften, Authentifizierungsmethode und Ähnliches. Diese Informationen werden über sogenannte Autorisierungsregeln verarbeitet, in denen festgelegt ist, welche Eigenschaften überprüft werden und welcher Zugriff gegebenenfalls erlaubt wird.

Dieser Bereich der Active Directory Federation Services können bei der Anbindung externer Benutzer in unseren Kommunikationsprozessen sehr hilfreich sein. Die Einrichtung ist aber nicht trivial. Insbesondere die Definition der Ansprüche erfordert Kenntnisse darüber, welche Informationen bei welchem Authentifizierungsverfahren in welcher Form übermittelt werden. Für einige Drittanbieter liefert wieder TechNet einige Informationen (*https://technet.microsoft.com/de-de/library/dn758113.aspx*) und auch Hinweise für die Erstellung eines eigenen Anbieters. Auch die Installation und Konfiguration wird hier wieder ausführlich beschrieben (*https://technet.microsoft.com/de-de/library/dn452410.aspx*).

3.2 SQL Server

SQL Server ist eine Serverkomponente zum Speichern und Verwalten relationaler Datenbanken, ein sogenanntes RDBMS (Relational DataBase Management System). In Microsoft-Umgebungen stellt der SQL Server eine Basistechnologie dar, die immer zum Einsatz kommt, wenn es darum geht, strukturierte Daten in großen Mengen zu speichern. Viele Anwendungen setzen daher eine Installation eines SQL Servers voraus, sei es als eigenständige Serverfarm im Unternehmen oder einfach als Dienst auf einem Anwendungsserver.

Schon bei der Darstellung der Active Directory Rights Management Services haben wir gesehen, dass diese ihrer Konfigurationsdaten in einer SQL-Datenbank speichern. Auch für SharePoint ist der SQL-Server eine Grundvoraussetzung. SharePoint speichert nicht nur seine Konfigurationsdaten, sondern auch alle Inhalte in SQL-Datenbanken.

Nicht alle Microsoft-Anwendungen, die relationale Datenbanken verwenden, nutzen allerdings den SQL Server als Basis. Zwei bekannte Ausnahmen sind das Active Directory und Exchange Server. Beide nutzen ein anderes Datenbanksystem (die sogenannte ESE-Engine), das schnellere Transaktionen erlaubt.

Neben der Speicherung der Datenbankanken bietet der SQL Server Auswertungskomponenten, die für einige unserer Kommunikationsprozesse interessant sind. Werfen wir zuerst einen Blick auf die Datenbankkomponente und danach auf die Analysis- und Reporting-Services.

3.2.1 SQL Server-Datenbank

Mit der Datenbankkomponente des SQL Servers werden wir bei der Gestaltung unserer Kommunikationsprozesse in der Regel nur indirekt in Berührung kommen. Wie einleitend erwähnt, nutzen einige der von uns eingesetzten Anwendungen diese Komponente als Daten-und Konfigurationsspeicher. Dabei werden die Datenbanken selbst bei der Installation beziehungsweise Konfiguration der Anwendungen von diesen automatisch erstellt. In den meisten Fällen ist ein direktes Bearbeiten der Datenbanken weder sinnvoll noch von Microsoft vorgesehen und kann zu einem Verlust des Herstellersupports führen.

Da diese Komponente von mehreren Anwendungen genutzt wird, macht es sich in der Regel schnell bezahlt, eine zentrale SQL Server-Infrastruktur im Unternehmen bereitzustellen. Damit lassen sich zentrale Backup- und Wiederherstellungsstrategien einrichten und ein hoher Grad an Ausfallsicherheit erreichen. Für die Einrichtung der Anwendungen sind der Name des Servers und die Authentifizierung für die Dienstkonten erforderlich. Der Zugriff auf die Daten der Anwendungen selbst erfolgt über definierte Dienstkonten. Diese müssen über entsprechende Berechtigungen auf die SQL Server-Instanzen verfügen. In der Regel sind die Berechtigungsstufen *dbcreator* und *securityadmin* für die Dienstkonten der Anwendungen erforderlich, um Datenbanken zu erstellen und die Berechtigungen an diesen zu vergeben. Alle weiteren Konfigurationen erfolgen in der Regel durch die Anwendungen selbst. Einige spezielle Konfigurationen möchte ich hier aber trotzdem beschreiben, da sie für die Arbeitsweise unserer Prozesse von Bedeutung sein können.

Werden in der Datenbank große Binärobjekte, sogenannte BLOBs (**B**inary **L**arge **OB**jects) abgelegt, zum Beispiel über ein Videoportal im SharePoint, kann es sinnvoll sein, das Feature des Filestream-Providers im SQL Server zu nutzen, um das Wachstum der Datenbanken einzuschränken und damit schnellere Transaktionen und vor allem effizientere Sicherungs- und Wiederherstellungsstrategien zu ermöglichen.

Über den Filestream-Provider werden große Dateien nicht mehr in der Datenbank selbst, sondern im Dateisystem gespeichert und in der Datenbank nur verlinkt. Für den Anwender ist dieser Vorgang nicht sichtbar. Die Dateien werden ganz normal als Inhalt der Datenbank präsentiert. Da der Pfad zur Ablage im Filestream-Provider angegeben werden kann, ermöglicht dieses Feature die Ablage der Inhalte auf einem dedizierten Laufwerk oder Platten-

array mit entsprechenden, optimierten Speicherungs- und Sicherungsmechanismen. Bei der Definition der Sicherungsverfahren für die Datenbank ist daran zu denken, diese Dateiablage mit zu sichern, um eine konsistente Wiederherstellung zu ermöglichen.

Gerade im Umfeld von SharePoint kann die SQL Server-Datenbank noch in anderer Form genutzt werden, als nur als Ablagesystem für eigene Inhalte. SharePoint ermöglicht es über sogenannte externe Inhaltstypen-Daten aus anderen Datenbanken abzufragen und über SharePoint-Funktionen zu bearbeiten. Auf SQL Server-Seite sind dafür die Mechanismen der Zugriffsteuerung zu beachten und die dafür nötigen Konfigurationen vorzunehmen.

Grundsätzlich kann SharePoint in einem solchen Szenario auf drei Arten auf die Datenbank zugreifen: mit dem Konto des angemeldeten Benutzers, mit seinem eigenen Dienstkonto oder mit einem vorher festgelegten Datenbankzugriffskonto. Häufig ist der erste Fall der am besten zu steuernde, da damit eine Berechtigungsüberprüfung für den angemeldeten Benutzer an der Datenbank erfolgt. Somit ist sichergestellt, dass tatsächlich nur berechtigte Benutzer die Inhalte der Datenbank in SharePoint auslesen können. Bei diesem Verfahren spricht man von einer Impersonation, das heißt, der SharePoint Server nimmt die Identität des Benutzers an und greift damit auf die Datenbank zu.

Bei Impersonationen gibt es eine Einschränkung, die als das Double-Hop-Szenario bekannt ist. Dahinter verbirgt sich die Tatsache, dass eine Impersonation in einem nicht-delegierbaren Anmeldeverfahren nur über einen Schritt, nicht über weitere Schritte möglich ist. Der erste Schritt ist die Impersonation des Clients, von dem aus der Benutzer zugreift. Dieser stellt die Verbindung zum SharePoint Server im Namen des Benutzers her. Wenn jetzt SharePoint im Namen des Benutzers auf einen weiteren Dienst zugreifen möchte, muss SharePoint vom Client die Anmeldedaten des Benutzers übernehmen. Dies schlägt fehl, wenn das Anmeldeverfahren keine Delegierung erlaubt.

Ein nicht delegierbares Anmeldeverfahren ist zum Beispiel die klassische Windows-Authentifizierung mittels Challenge-Response (auch als NTLM-Verfahren bekannt). Ein delegierbares Anmeldeverfahren ist das über Tickets und Tokens arbeitende Kerberos-Verfahren. Beides sind mögliche Anmeldeverfahren für SharePoint-Webanwendungen. Bei der Erstellung einer Webanwendung muss entschieden werden, welches der beiden Verfahren für die Anmeldung der Benutzer genutzt werden soll. Wenn Zugriffe auf Drittsysteme über SharePoint vorgesehen sind, bietet es sich an, von vornherein auf Kerberos zu setzen. Dieses erfordert einige zusätzliche Konfigurationen in der Domäne:

1. Den Dienstkonten der SharePoint-Webanwendungen und des SQL Servers muss „Für Delegierungszwecke vertraut“ werden. Dies ist eine Option in den erweiterten Einstellungen des Benutzerkontos.
2. Für die Dienstkonten der SharePoint-Webanwendungen müssen Dienstprinzipalnamen (Service Principal Names, SPNs) für http sowohl auf den Hostnamen als auch den FQDN (Vollqualifizierter Domänenname, DNS-Name) des SharePoint-Servers bzw. der Web-Anwendung gesetzt werden.
3. Für die Dienstkonten des SQL Servers muss ein SPN auf das SQL-Protokoll gesetzt werden.

In den aktuellen Versionen von SharePoint Server (2013 und 2016) und SQL Server (2012, 2014 und 2016) ist die Einrichtung der Kerberos-Authentifizierung für einige Szenarien nicht mehr erforderlich, da SharePoint Server einen eigenen Token-Dienst installiert, der

die klassischen Anmeldeinformationen des Benutzers in ein Ticket umwandelt, das vom SQL Server akzeptiert wird. Es gibt aber immer noch Szenarien, die eine Kerberos-Authentifizierung erfordern, insbesondere dann, wenn das Zielsystem die SharePoint-Tickets nicht interpretieren kann.

Zwei weitere Einstellungen beim Einrichten der Verbindung zum SQL Server im SharePoint können ebenfalls hilfreich sein.

Abhängig vom eingesetzten Hochverfügbarkeitsszenario des SQL Servers, bietet der SharePoint die Möglichkeit, einen alternativen Datenbankserver zu benennen, auf den zugegriffen wird, wenn der primäre nicht verfügbar ist. Dieser lässt sich sehr gut in Kombination mit den sogenannten Log-Shipping-Verfahren im SQL Server einsetzen (*https://msdn.microsoft.com/en-us/library/ms187103.aspx*). Dabei handelt es sich um ein Ausfallsicherungsverfahren, das auch in den neueren Versionen von SQL Server noch eingesetzt werden kann, auch wenn es inzwischen von Microsoft als „deprecated“ eingestuft wurde.

Eine weitere, sehr hilfreiche Konfiguration ist die Nutzung von SQL-Aliasen für die Verbindungen zum SQL Server. Dabei wird auf dem Anwendungsserver, zum Beispiel dem SharePoint Server im SQL Client ein virtueller, aber statischer Name für den SQL Server eingetragen, der auf den tatsächlichen Namen des SQL Servers verweist. Dieser Alias wird in den Verbindungseinstellungen des Anwendungsservers genutzt. Da der SQL-Alias kein öffentlicher Name ist, sondern nur auf dem Anwendungsserver selbst bekannt ist, kann sich der tatsächliche Name des SQL Servers ändern, z. B. wenn die Datenbank auf einen anderen Datenbankserver verschoben wird, ohne dass sich der Name in den Verbindungseinstellungen von SharePoint ändern muss. Nur der Verweis im Alias wird geändert und die Datenbank wird über den Alias wiedergefunden. Dies ist insbesondere dann hilfreich, wenn die Anwendung sehr viele Datenbanken pflegt, wie gerade SharePoint Server, da dann die Verbindung bei Änderungen nur an einer Stelle bearbeitet werden muss, und nicht für jede eingebundene Datenbank.

3.2.2 SQL Server Analysis Services

Während die Datenbankkomponente des SQL Servers eher ein Dienst ist, den wir als Basis für unsere Kommunikationsanwendungen benötigen, sind die beiden folgenden Komponenten, die Analysis Services und die Reporting Services, spezielle Kommunikationskomponenten, die insbesondere in vertikalen Kommunikationsprozessen zur Anwendung kommen. Beide dienen in gewisser Weise dazu, Informationen zu aggregieren und auszuwerten. Beginnen wir mit der Betrachtung der Analysis Services.

Bei den SQL Server Analysis Services (SSAS) handelt es sich um die Implementierung eines OLAP-Werkzeuges (OLAP steht für OnLine Analytical Processing) in der Microsoft-Datenbankplattform. Wie der Name schon deutlich macht, dient es der ad-hoc-Analyse großer Datenmengen. Dazu werden die Daten in den Tabellen und Datenbanken über sogenannte OLAP-Cubes zueinander in Beziehung gesetzt. OLAP-Cubes sind multidimensionale Datenbanken. Es werden aus den Daten Dimensionen extrahiert, die für die Aggregation der Daten genutzt werden. Die aus Excel bekannte Pivot-Funktion repräsentiert im Grunde genommen dasselbe Verfahren für die Umwandlung einer einzelnen Tabelle in eine zweidimensionale Datenbank. Stellen Sie sich eine Liste von Umsatzdaten mit Informationen

über Beträge, Datumsangaben, Kunden, Produkte usw. vor. Diese Daten können aus verschiedenen Tabellen kommen und in einer Ansicht zusammengeführt werden. Dann liegen sie aber immer noch in Form einer flache Liste vor (vgl. Bild 3.3), die zwar nach mehreren Kriterien gefiltert werden kann, bei der aber die Zusammenfassung der Daten nach verschiedenen Kriterien aufwändig ist, zum Beispiel um eine Frage zu beantworten wie: „Welches Produkt verkauft sich an welchem Ort am besten?“

	A	B	C	D	E	F	G	H
1	Verkaufsdatum	Kunde	Ort	Produkt	Kategorie	Anzahl	Einzelpreis	Summe
2	01.01.2015	Meier	Essen	Sosta	Buch	7	7,85 €	54,95 €
3	10.01.2015	Schulze	Frankfurt	Ferienfieber	Poster	2	12,60 €	25,20 €
4	19.01.2015	Müller	Mülheim	Farbentraum	Poster	1	5,40 €	5,40 €
5	28.01.2015	Klausen	Karlsruhe	Domenica	Foto	3	3,80 €	11,40 €
6	06.02.2015	Hansen	München	Sosta	Buch	5	7,85 €	39,25 €
7	15.02.2015	Franz	Essen	Ferienfieber	Poster	7	12,60 €	88,20 €
8	24.02.2015	Breitwieser	Frankfurt	Farbentraum	Poster	9	5,40 €	48,60 €
9	05.03.2015	Meier	Mülheim	Domenica	Foto	8	3,80 €	30,40 €
10	14.03.2015	Schulze	Karlsruhe	Sosta	Buch	7	7,85 €	54,95 €
11	23.03.2015	Müller	München	Ferienfieber	Poster	6	12,60 €	75,60 €

Bild 3.3 Die Daten als flache Tabelle

Dafür muss die Liste zumindest so angeordnet werden, dass die Orte in den Zeilen abgetragen werden und die Produkte in den Spalten. In den Zellen der Tabelle können dann die Anzahl der verkauften Produkte aufsummiert werde. Das ist die Funktionsweise einer Pivot-Tabelle in Excel (vgl. Bild 3.4).

Summe von Anzahl	Spaltenb							
	Buch	Buch	Foto	Foto	Poster		Poster	Gesamt
Zeilenbeschriftungen	Sosta		Domenica		Farbentraum	Ferienfieber		
Essen	19	19	7	7	14	11	25	51
Frankfurt	7	7	13	13	14	8	22	42
Karlsruhe	14	14	5	5	11	7	18	37
Mülheim	10	10	14	14	5	7	12	36
München	8	8	14	14	7	14	21	43
Gesamtergebnis	**58**	**58**	**53**	**53**	**51**	**47**	**98**	**209**

Bild 3.4 Dieselben Daten in der Pivot-Auswertung

Wenn die ursprüngliche Frage nun um den Verkaufszeitpunkt erweitert wird, also: „Welches Produkt verkauft sich an welchem Ort in welchem Monat am besten?“, wird eine zusätzliche, die dritte Dimension benötigt. Man kann sich das so vorstellen, als ob in dem Beispiel jetzt für jede Zeiteinheit eine eigene Tabelle hinterlegt würde und die Zellen, in denen das Produkt und der Ort zusammenfasst werden, jetzt über alle Tabellen hinsichtlich der Zeit abgefragt werden können (praktisch in den Würfel stechen). Dies ist eine mehrdimensionale Datenabfrage. Bei großen Datenmengen können natürlich noch weitere Dimensionen hinzukommen, wie zum Beispiel Niederlassungen, Abteilungen und Mitarbeiter. Um diese Dimensionen abzufragen, werden OLAP-Cubes eingesetzt, als Würfel, die aus mehr als drei Dimensionen bestehen.

Dimensionen in OLAP-Cubes zeichnen sich dadurch aus, dass sie skalierbar sind. Zeitdimensionen lassen sich auf Tage, Wochen, Monate, Quartale, Jahre etc. zusammenfassen beziehungsweise auch wieder zerlegen. Bricht man eine Dimension bis zum einzelnen Datensatz herunter, um zum Beispiel zu sehen, welche Verkäufe hinter den Monatsumsätzen des Januars in Karlsruhe stehen, spricht man von einem Drilldown in der Datenbank.

Man mag sich vielleicht fragen, was das mit unseren Kommunikationsprozessen zu tun hat. Sehr viel, sage ich. Die Daten, die wir hier abfragen, kommen nämlich klassischerweise aus den Kommunikationsprozessen wie zum Beispiel dem Unternehmensreporting. Der Vertrieb liefert zum Beispiel die Informationen über Angebote und Verkäufe, indem er sie in ein Datenbankformular einträgt und als Datensatz speichert. Das Controlling fragt diese Daten in einem monatlichen Bericht ab, fügt eventuell noch Vormonats- und Vorjahresvergleiche hinzu und liefert das Ganze als Report an die Geschäftsführung. Was ist das, was wir da beschrieben haben? Ein vertikaler, asynchroner und aggregierender Kommunikationsprozess! Damit dieser funktioniert, müssen wir die Ziele kennen, die damit erreicht werden sollen. Wir müssen also wissen, welche Informationen die Geschäftsführung benötigt. Dann können wir diesen Prozess rückwärts planen, indem wir schauen, wie diese Daten aggregiert werden und welche Daten die Vertriebsberichte liefern müssen, damit die Aggregation auch funktioniert und die richtigen Ergebnisse liefert. Damit können wir dann die Dateneingabe für den Vertrieb gestalten.

Da die Aggregation mithilfe der Analysis Services erfolgen kann, werden diese ein zentraler Bestandteil des Kommunikationsprozesses. Die Gestaltung der Abfragen und die Bildung der Cubes ist in der Regel Aufgabe von Spezialisten. Bei der Gestaltung der Prozesse müssen wir aber wissen, wie wir die Daten in unseren Prozessen zuliefern können, und wie wir sie auf der anderen Seite abfragen können.

3.2.3 SQL Server Reporting Services

Während die SQL Analysis Services die Daten für die Auswertung vorbereiten, dienen die SQL Server Reporting Services (SSRS) dazu, die Daten zu präsentieren. Hinter den Reporting Services steht ein Abfragemodell, das Daten aus verschiedenen Quellen zeitgesteuert oder ad hoc abfragt und in Form von Berichten darstellt. Diese Berichte können Tabellen, Diagramme oder Leistungsindikatoren enthalten. Die Daten selbst können aus relationalen Datenbanken, multidimensionalen OLAP-Cubes oder aus XML-Daten stammen. Ziel ist es, Daten schnell erfassbar und lesbar darzustellen.

Der Aufbau der Berichte erfolgt auf mehreren Ebenen. Zuerst müssen die Datenquellen erfasst und definiert werden. Dabei sind neben Art und Namen der Datenquelle unter anderem auch die Zugriffsinformationen anzugeben.

Aus den Datenquellen werden sogenannte Datasets erzeugt, die die abzufragenden Daten umfassen. Diese werden wiederum über Berichtsparameter in spezifischer Form ausgewertet, also zum Beispiel gefiltert oder zusammengefasst. Außerdem können über die Berichtsparameter Berechtigungen auf Teile des Berichtes gesetzt werden.

Die Daten werden schließlich in verschiedenen Datenbereichen und Karten des Berichts dargestellt. Dies können Tabellen, Listen, Matrizen, Indikatoren oder Karten sein. Aus den

Elementen des Berichtes können Berichtsteile definiert werden, die dann wiederum einzeln veröffentlich werden können. Über die Veröffentlichung einzelner Berichtsteile kann sichergestellt werden, dass Daten nur berechtigen Benutzern zugänglich gemacht werden.

Das gesamte Design des Berichtes wird in XML-basierten Berichtsdefinitionen (.rdl oder .rdlx-Dateien) gespeichert. Zu den Berichtsdefinitionen können Zeitpläne hinzugefügt werden, die dafür sorgen, dass der Bericht regelmäßig neu erstellt wird. Die Darstellung der Berichte erfolgt schließlich in Dateiform, als HTML-Datei (eine Webseite) oder als PDF.

Die SQL Reporting Services können als eigenständige Berichtsplattform im Unternehmen eingesetzt werden, um zum Beispiel eine zentralisierte Datenauswertung zu ermöglichen. Für unsere Kommunikationsprozesse ist aber die zweite Einsatzvariante hilfreicher, nämlich die Integration der Reporting Services in SharePoint. Dieser Integrationsmodus – es handelt sich dabei um einen eigenen Installationsmodus der Reporting Services – ermöglicht den Zugriff auf die Berichte und die Darstellung der Berichte in einer für den Anwender homogenen Umgebung.

Für die Integration sind die Unterstützungskomponenten für die SSRS auf dem SharePoint Server zu installieren und die Verbindung zum Reporting Server zu definieren. Danach können Berichtsbibliotheken genutzt werden, um Berichtsdefinitionen und Zeitpläne zu speichern und zu veröffentlichen. Die Ergebnisdarstellungen können anschließend als Webseiten veröffentlicht werden. Sehr hilfreich sind die Reporting Services im Rahmen der Nutzung der Business-Intelligence-Komponenten in SharePoint, insbesondere den Performance Point Services. Deren Dashboards können verschiedene Komponenten aus den Reporting Services enthalten.

Auch hierbei handelt es sich um eine Auswertungskomponente, die vor allem in aggregierenden Kommunikationsprozessen eingesetzt werden kann. Ziel der Reporting Services ist aber nicht die Organisation der Daten an sich (dafür bieten sich unter anderem die Analysis Services an), sondern die effiziente Darstellung der Auswertungsergebnisse. Sie bieten somit die Möglichkeit, die Verständlichkeit der Kommunikation – insbesondere bei der Auswertung numerischer Daten – zu erhöhen. Durch die Einbindung in SharePoint kann diese Darstellung praktisch nahtlos mit Kommunikationsprozessen verbunden werden.

3.3 SharePoint Server

Eine der zentralen Plattformen für die Gestaltung von Kommunikationsprozessen bildet sicherlich SharePoint. Durch seinen Funktionsumfang und die starke Integration in andere Anwendungen stellt der SharePoint Server die zentrale Schaltstelle vieler Kommunikationsprozesse dar. Neben der Teamkommunikation und Veröffentlichungsmechanismen bietet er insbesondere eine Workflowkomponente, Formulardienste und Business-Intelligence-Funktionen (BI-Funktionen), die in Kommunikationsprozessen genutzt und zusammengeführt werden können. In keiner anderen Anwendung wird der Integrationsgedanke so sichtbar wie im SharePoint. Über die Datenverbindungen lassen sich Daten aus verschiedensten Quellen einbinden und mit nativen SharePoint-Daten verknüpfen. Die Daten können vom Anwender in Office-Anwendungen genutzt und analysiert werden und die Ergebnisse wie-

derum im SharePoint veröffentlicht werden. Dabei sind Funktionen wie Benachrichtigungen und Genehmigungsverfahren schon als Standards ebenso verfügbar wie klassische Dokumentenmanagementwerkzeuge. Die folgende Beschreibung kann daher die verschiedenen Funktionen nur grob anreißen. Ein Buch über alle Einsatzszenarien dieses Produkts würde sicherlich anderthalb bis zweitausend Seiten umfassen. Ich werde aber in der Umsetzung einige zentrale Einsatzszenarien ansprechen.

3.3.1 SharePoint-Basisfunktionen

Je nachdem, von welcher Seite man das Produkt SharePoint betrachtet, findet man unterschiedliche Beschreibungen. So kann man es als einen dynamischen Webserver, ein Kollaborationswerkzeug, eine Buisness Intelligence Plattform, ein Content Management System, ein Werkzeug für die Unternehmenssuche oder auch ein Datenintegrationswerkzeug beschreiben. Ich bevorzuge tatsächlich den letzten Begriff, da er der Bandbreite der Einsatzmöglichkeiten am ehesten gerecht wird.

Basis aller Funktionen das SharePoint ist die Kollaborationsplattform. Dies erkennt man schon daran, dass diese Grundfunktionen in Form der SharePoint Foundation (bis Version 2013) von Microsoft lizenzkostenfrei angeboten werden. Teams arbeiten im SharePoint auf einer Website zusammen. Websites können wiederum Unterwebsites enthalten. Die Grundstruktur des SharePoint ist daher eine Hierarchie von Websites, in der zum Beispiel ein Geschäftsbereich eine Website zur Zusammenarbeit bekommt, darin jede Abteilung wieder eine eigene Website, in denen wiederum einzelne (Projekt-)Teams eigene Websites haben. Die Website auf der obersten Ebene bildet die Websitesammlung. Diese ist ein administrativer Kontext, der von einem begrenzten Personenkreis administriert wird (den sogenannten Websitesammlungsadministratoren). Bestimmte Funktionen in SharePoint können nur auf Websitesammlungsebene verwaltet werden, zum Beispiel Websitevorlagen (sogenannte Lösungen oder Solutions). Die Websitesammlungen, von denen es auch mehrere innerhalb einer Hierarchie geben kann, sind wiederum Bestandteil einer Webanwendung. Die Webanwendung repräsentiert die eher technische Sicht auf den SharePoint. Hier werden unter anderem die Authentifizierungsverfahren festgelegt, mittels der sich Benutzer am SharePoint anmelden können, und weitere Funktionen, wie die Einschränkungen der Massenverarbeitung von Listenelementen. Die oberste Ebene des SharePoint stellt schließlich die Serverfarm dar, bestehend aus Datenbankservern, Anwendungsserver und Web-Servern (sogenannten Web-Frontends).

Innerhalb einer Website werden alle Inhalte in SharePoint in Listen und Bibliotheken verwaltet. Es gibt keine Inhalte, die nicht in irgendeiner Form von Liste oder Bibliothek vorliegen. Für viele Standardfunktionen kennt SharePoint vorkonfigurierte Listenvorlagen wie Kalenderlisten, Problemverfolgungslisten, Aufgabenlisten, Kontaktlisten und Bibliotheksvorlagen in Form von Dokumentbibliotheken, Bildbibliotheken, Formularbibliotheken etc. Welche Vorlagen und Listentypen verfügbar sind, ist abhängig von den aktivierten Features beziehungsweise der beim Erstellen der Website verwendeten Websitevorlage. Typische Websitevorlagen sind die Teamwebsite, eine Projektwebsite oder auch ein Veröffentlichungsportal. Gerade Veröffentlichungswebsites zeichnen sich durch eine Reihe spezieller Funktionen aus, die wir uns im Bereich des Marketings später in der Umsetzung genauer anschauen werden.

Listen enthalten Elemente, Bibliotheken Dokumente oder Dateien. In beiden können die Elemente wiederum in Ordnerstrukturen abgelegt werden. Die Darstellung der Listeninhalte erfolgt mittels Ansichten. In Ansichten können die Elemente gefiltert und sortiert oder in spezifischer Form abgebildet werden. Die Ansichten wiederum können in Webseiten als sogenannte App-Webparts eingebunden werden, so dass verschiedene Elemente wie Adressinformationen von Ansprechpartnern und Dokumente zu diesen Ansprechpartnern auf einer Webseite dargestellt werden können.

Neben App-Webparts gibt es weitere Webparts in SharePoint, über die spezifische Funktionen wie Excel-Diagramme, Filterfunktionen, Bildvorschauen bis hin zu spezifischen Codeelementen in eine Seite eingebunden werden können.

Die gesamte Hierarchie einer SharePoint-Installation stellt sich wie folgt dar (Bild 3.5):

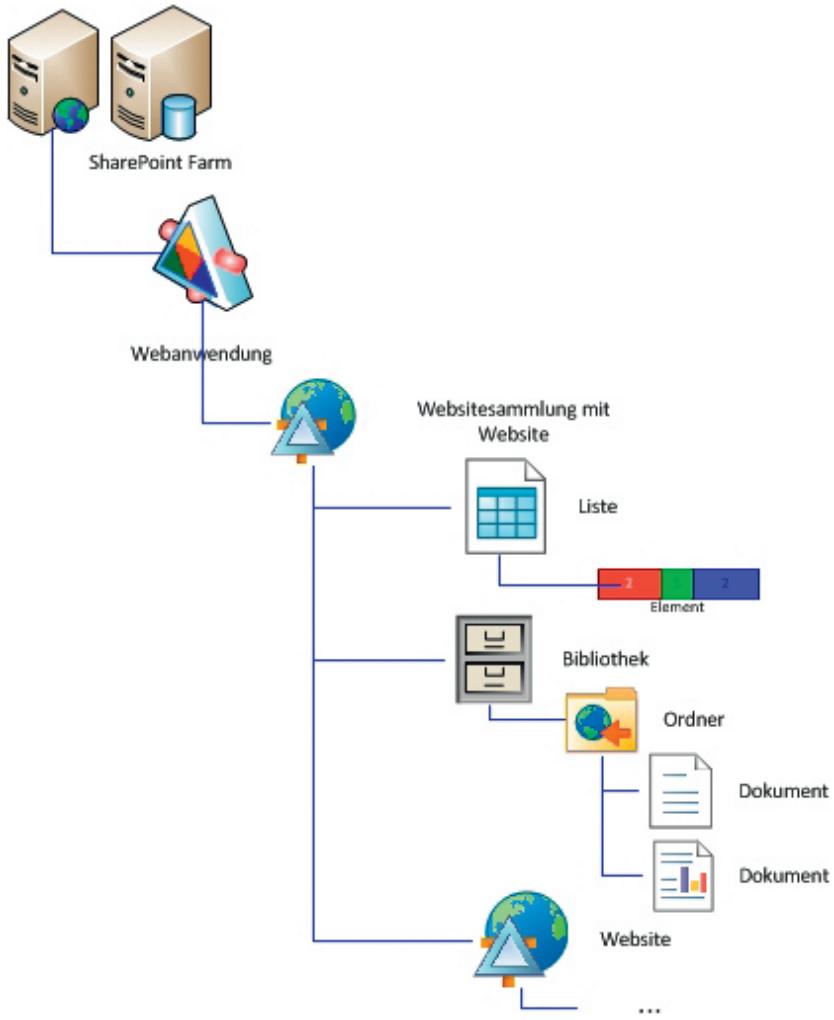

Bild 3.5 Die SharePoint-Hierarchie

Beim Aufbau einer solchen Websitehierarchie sind in SharePoint einige Einschränkungen zu berücksichtigen:

- Verlinkungen zwischen Listen über Nachschlagefelder sind nur innerhalb einer Website möglich.
- App-Webparts sind nur für die Listen der eigenen Website verfügbar.
- Die Berechtigungsverwaltung in SharePoint folgt dieser Hierarchie, ausgehend von den Berechtigungen der Websitesammlungen. Dabei verfolgt SharePoint ein rollenbasiertes Berechtigungsmodell, bei dem Benutzer zu Gruppen zusammengefasst werden. Den Gruppen können auf den verschiedenen Ebenen Berechtigungsstufen zugewiesen werden, die definieren, welche Aktionen die Benutzer ausführen dürfen. Beim Anlegen einer Website werden drei Standardbenutzergruppen eingerichtet, *Besitzer*, *Besucher* und *Mitglieder* der Website (bei Veröffentlichungswebsites noch weitere). Diesen werden die Berechtigungsstufen *Vollzugriff*, *Lesen* und *Bearbeiten* vergeben. Während *Vollzugriff* volle Verwaltungsrechte innerhalb der Website (nicht unbedingt der Websitesammlung) gewährt und *Lesen* nur lesenden Zugriff ermöglicht, können die Mitglieder mit *Bearbeiten*-Zugriff Elemente erstellen, bearbeiten und löschen und auch eigene Listen auf der Website anlegen.
- Das Berechtigungsmodell im SharePoint sieht grundsätzlich wie folgt aus (Bild 3.6):

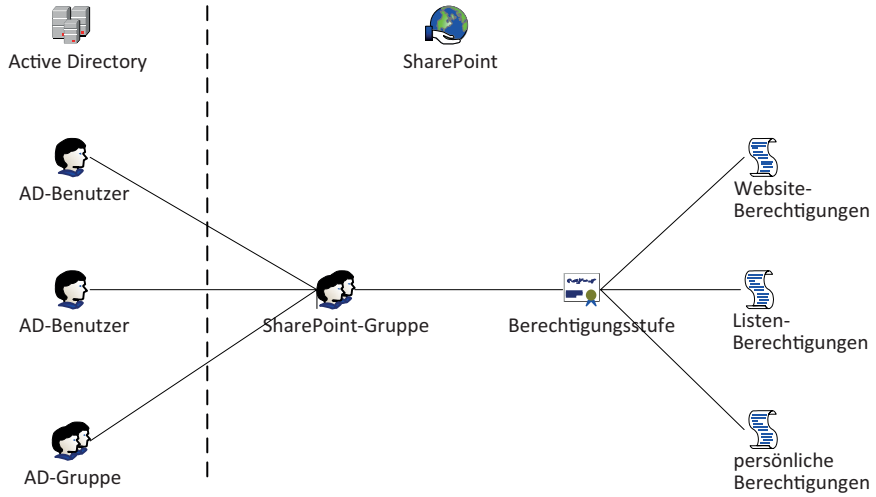

Bild 3.6 Das SharePoint-Berechtigungsmodell

Auch unter dem Aspekt der Berechtigungsvergabe sind einige spezifische Einschränkungen in der Hierarchieplanung zu beachten.

- SharePoint-eigene Benutzergruppen werden auf der Ebene der Websitesammlung angelegt und können nur innerhalb derselben Websitesammlung verwendet werden (das gilt nicht für Active-Directory-Gruppen, denen im SharePoint überall Berechtigungen gegeben werden können).
- Innerhalb der Websitesammlung werden die Berechtigungen standardmäßig von oben nach unten vererbt, das heißt die Berechtigungen, die auf Websitesammlungsebene angelegt sind, gelten auch auf die einzelnen Dokumente innerhalb untergeordneter Websites.

- Die Vererbung kann auf jeder Ebene unterbrochen werden. Die unterste Berechtigungsebene ist die Elementebene.
- Berechtigungen werden in SharePoint über Berechtigungsstufen vergeben. Diese werden ebenfalls auf Websitesammlungsebene verwaltet und können auch nur von Administratoren dieser Ebene geändert werden.

Schon die SharePoint Foundation (in Version 2013) bietet neben den klassischen Teamfeatures auch eine ausgefeilte Suchfunktion. Die Suchfunktion von SharePoint basiert auf einer Volltextindizierung aller lesbaren Inhalte innerhalb der Website. Dazu gehören auch die in den Bibliotheken liegenden Dokumente. Neben seinen eigenen Inhalten kann SharePoint aber auch noch weitere Speicher des Unternehmens durchforsten, zum Beispiel Dateifreigaben, Datenbanken, auf die er mit den Business Connectivity Services (BCS) zugreifen kann, Lotus-Notes-Datenbanken und andere Websites.

Bei der Indizierung werden die Berechtigungen auf die Inhalte, soweit sie von SharePoint lesbar sind, festgehalten. Dadurch ist sichergestellt, dass Benutzer auch mit der Suche nur auf die Inhalte zugreifen können, auf die sie berechtigt sind. Dies setzt aber insbesondere in Dateifreigaben voraus, dass Berechtigungen explizit gepflegt werden. Nicht in allen Unternehmen ist das der Fall. Häufig werden Freigaben einfach „versteckt“, ohne den Zugriff über Berechtigungen einzuschränken. Sobald solche Inhalte über die SharePoint-Suche verfügbar werden, kann das zu nicht gewollten Ergebnissen führen.

3.3.2 Excel und Visio Services

Mit den höheren Lizenzen von SharePoint werden weitere Funktionen verfügbar. Einige davon sind für unsere Kommunikationsprozesse von besonderer Bedeutung.

Ein häufig eingesetztes Feature in der Enterprise-Lizenz von SharePoint sind die Excel Services und in Teilen auch die Visio Services, wobei letztere seltener angewendet werden. Beide Dienste arbeiten nach demselben Prinzip. Excel oder Visiodateien werden über Webparts in eine Webseite eingebunden und die in der jeweiligen Datei liegenden Berechnungen und Datenabfragen online aktualisiert.

Dabei können alle Funktionen, die Excel und Visio für die Datenauswertung kennen, genutzt werden, inklusive Pivotauswertungen. Hilfreich ist zudem, dass beide Anwendungen die Möglichkeit bieten, auf externe Daten zuzugreifen, zum Beispiel auf SharePoint-Listen.

Damit bekommen Anwender eine einfache Möglichkeit, Auswertungen in bekannten Werkzeugen vorzunehmen, die Ergebnisse gleichzeitig anderen Benutzern direkt zur Verfügung zu stellen. So lassen sich einfache BI-Funktionen effizient und schnell implementieren.

Zwar benötigen beide Dienste einige grundlegende Konfigurationen, diese sind aber nicht problematisch. In erster Linie ist in den Diensteinstellungen festzulegen, welche Daten als vertrauenswürdig angesehen werden, damit sie über die Services aktualisiert werden können.

Seit SharePoint 2016 werden Excel Services nicht mehr als Dienstanwendung in SharePoint betrieben. Die entsprechenden Funktionen werden jetzt über Office Online Server zur Verfügung gestellt. Weiterhin sind aber Excel-Webparts zur Darstellung von Excel-Dateien auf einer SharePoint-Website verfügbar.