Arnold Picot · Udo Hertz · Thomas Götz
Herausgeber

Trust in IT

Wann vertrauen Sie Ihr Geschäft der Internet-Cloud an?

Springer

Herausgeber
Prof. Dr. Dr. Arnold Picot
Universität München
Institut für Information,
Organisation und Management
Ludwigstr. 28
80539 München
Deutschland
picot@lmu.de

Udo Hertz
IBM Deutschland
Director of Information
Management Development
Schönaicher Str. 220
71032 Böblingen
Deutschland
udo.hertz@de.ibm.com

Dr. Thomas Götz
Partner
Strategy & Transformation Management Consulting
IBM Global Business Services
Karl-Arnold-Platz 1 A
40474 Düsseldorf
Deutschland
thomas.goetz@de.ibm.com

ISBN 978-3-642-18109-2 e-ISBN 978-3-642-18110-8
DOI 10.1007/978-3-642-18110-8
Springer Heidelberg Dordrecht London New York

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

Einbandentwurf: WMXDesign GmbH, Heidelberg

Gedruckt auf säurefreiem Papier

Springer ist Teil der Fachverlagsgruppe Springer Science+Business Media (www.springer.com)

Vorwort

Es gibt kaum ein Thema in der IT-Branche, das in der letzten Zeit so viel Aufmerksamkeit erregt hat wie Cloud Computing. Analysten wie Unternehmen sind sich einig: Cloud ist der nächste Paradigmenwechsel in der IT – weg von starren IT-Infrastrukturen für Unternehmen und Konsumenten hin zur dynamischen Nutzung von „IT-Ressourcen aus der Wolke“. Beim Cloud Computing nutzen Unternehmen Hardware, Software und Services über ein Netzwerk dynamisch und nach Bedarf, um ihre IT effizienter einzusetzen und Kosten zu senken.

Im Internet entstehen mit Angeboten wie „Software as a Service“ neue Möglichkeiten für Unternehmen und private Nutzer, die die Installation, den Betrieb von Anwendungen sowie die Speicherung der anfallenden Daten auf eigenen, lokalen Rechnern zunehmend ablösen und IT damit flexibler und kostengünstiger gestalten. Doch spätestens wenn geschäftskritische, sensible Daten eines Unternehmens oder auch private Daten von Bürgern in einer öffentlichen Cloud betrieben werden sollen, stehen Fragen zu Verfügbarkeit, Sicherheit und vor allem Vertrauen im Raum:

- Was passiert, wenn ein Unternehmen seine IT-Infrastruktur und Anwendungen von einem entsprechenden Anbieter bezieht und der die Leistung einstellt oder dauerhaft nicht mehr bereitstellen kann?
- Welche Handhabe hat man, wenn der Anbieter im Ausland seinen Firmensitz hat?
- Unter welchen Bedingungen würden Firmen ihre unternehmenskritischen Anwendungen und Daten IT-Versorgern über das Internet anvertrauen?
- Welche besonderen Anforderungen stellen sich an das Konzept Cloud Computing?
- Braucht es weltweite Aufsichtsbehörden für dieses Geschäftsfeld?

Die Fachkonferenz hat Antworten auf diese und weitere Fragen gesucht. Diese Fragen sind letztlich – wie wir aus unserer Zukunftsstudie wissen – eng mit der Vertrauensproblematik in der Informationsgesellschaft, einem Kernthema der Zukunft, verknüpft.

Im vorliegenden Band sind die Vorträge und die durchgesehene Mitschrift der Podiumsdiskussion enthalten. Allen Referenten und Diskussionsleitern sowie all denen, die zum Gelingen der Konferenz und zur Erstellung dieses Buches beigetragen haben, gilt unser Dank.

Arnold Picot Thomas Götz Udo Hertz

Inhalt

1 Begrüßung

Prof. Dr. Arnold Picot
Ludwig-Maximilians-Universität München

Meine sehr geehrten Damen und Herren, ich habe die Freude, Sie heute Morgen begrüßen zu dürfen. Wir freuen uns, dass trotz einiger widriger Umstände – Warnstreiks, Wetter – so viele Teilnehmer kommen konnten.

„Trust in IT – Wann vertrauen Sie Ihr Geschäft der Internet Cloud an?“ ist das Thema unserer Tagung. Über dieser Tagung steht das Thema Vertrauen, Vertrauen in Wirtschaft und Gesellschaft, insbesondere in den Branchen und Dienstleistungssektoren, mit denen wir es hier zu tun haben, nämlich in Information, Kommunikation und Medien.

Was ist nun Vertrauen? Es gibt vielleicht so viele Definitionen von Vertrauen wie Fachleute hier im Saal versammelt sind. Allerdings haben die meisten Definitionen einen gemeinsamen Kern. Dieser Kern der Definition und des Begriffs „Vertrauen“ bedeutet, dass Vertrauen eine riskante Vorleistung beinhaltet. Sie wird in der Erwartung geleistet, dass dieser Vorleistung von der Gegenseite entsprochen wird. Ich lege Geld bei einer Bank an (riskante Vorleistung) in der Erwartung, dass die Bank damit den Vereinbarungen entsprechend sowie professionell umgeht. Ich erteile einem Handwerker, u.U. mit gleichzeitiger Anzahlung, einen Auftrag in der Erwartung, dass er eine Reparaturdienstleistung zeit- und fachgerecht ausführt. Man geht also dauernd im geschäftlichen wie im privaten Leben, in nahezu allen Beziehungen, Risiken durch Vorleistung ein. Dabei baut man darauf, dass die andere Seite sich so verhält, wie man es sich vorstellt, wie man es geäußert hat oder auch nur meint vereinbart zu haben oder unterstellen zu können.

Diese Art von riskanten Vorleistungen treten bei nahezu allen sozialen Interaktionen und wirtschaftlichen Transaktionen auf, besonders dann, wenn Leistung und Gegenleistung zeitlich und räumlich auseinanderfallen, wenn sie also nicht sozusagen uno actu an einem Ort und in einem Moment realisierbar sind. Das ist bei den meisten unserer Interaktionen, Beziehungen und Transaktionen der Fall, weil es eben keine simultane Abstimmung von Leistung und Gegenleistung gibt. Vielmehr werden viele Leistungsbeziehungen über die Zeit gestreckt. Sie werden als Leistungsversprechen gegeben, die zumindest teilweise erst später eingelöst werden. Somit entsteht eine Lücke, die manchmal in Teilen durch rechtliche Sanktionen oder Sicherheiten gefüllt werden kann, deren verbleibender Rest aber nur durch Vertrauen zu überbrücken ist, da ansonsten die Beziehung nicht zustande käme. Es

A. Picot et al. (eds.), *Trust in IT*, DOI 10.1007/978-3-642-18110-8_1,

gibt in unserer Welt wohl keine Vereinbarung, keinen Vertrag, der vollständig wäre und damit alle Aspekte abdeckt, die unter Risikogesichtspunkten abzudecken wären. Insofern sind fast alle Vereinbarungen unvollständig. Immer, wenn es um Beziehungen geht, die nur unvollständig vereinbart sind, aber Lücken aufweisen, müssen wir diese Lücken schließen, sonst kann Kooperation nicht gelingen. Vertrauen ermöglicht das Schließen der Lücken. Es besteht in der erwähnten riskanten Vorleistung, die jemand erbringen muss, damit die Leistungsbeziehung in Gang kommt.

Wer zum Arzt geht und ihm seine Probleme anvertraut und darauf vertraut, dass Medikation oder Therapie richtige sind, wer einem Händler oder Lieferanten seine Wünsche anvertraut, mit einem Handwerker einen Vertrag eingeht, wer ein Eheversprechen abgibt – stets ist eine riskante, auf Vertrauen setzende Vorleistung im Spiel. Und natürlich ist es auch im Bereich der Informations- und Kommunikationstechnologien und ihrer Services so, die machen da keinerlei Ausnahme.

Während wir noch vor einigen Jahren und Jahrzehnten eine ausgesprochene hoheitliche Konzentration der informations- und kommunikationstechnischen Aktivitäten bei den jeweiligen anwendenden Organisationen und wenigen Lieferanten hatten, haben sich die Märkte in der Zwischenzeit ausdifferenziert und wir bieten vielfältige spezialisierte Dienstleistungen an, aus denen der Anwender seine Lösung zusammenstellt. Die Märkte werden größer, so dass sich die Spezialisierung lohnt. Immer mehr Services und immer mehr Transaktionen in den IKT- Bereichen werden auf arm's length, wie wir sagen, also in einer gewissen Distanz zum Leistenden abgewickelt, also nicht in Symbiose zwischen Auftraggeber und Auftragnehmer, sondern außerhalb des eigenen Hoheits- und Kontrollbereichs.

In diesem Zusammenhang werden zahlreiche persönliche, geschäftliche und finanzielle Daten zur Aufbereitung, Aufbewahrung und Weiterverarbeitung Dritten übergeben. Das ist im Prinzip nichts Neues, das gab es in vielen Bereichen von Wirtschaft und Gesellschaft immer schon. Aber nun nehmen im Zuge der Digitalisierung Vielfalt, Volumen und Schnelligkeit des Datenaustauschs sprunghaft zu. Wir müssen uns fragen, wer die Partner sind, mit denen wir zusammenarbeiten. Wo lagern die Daten? Wo sind die Programme und wie funktionieren sie, wie verläuft diese Verarbeitung?

Die Partner, die solche Verarbeitungs-, Aufbewahrungs- und Austauschprozesse abwickeln, sind in manchen Fällen klar identifizierbar, und in anderen Fällen ist es nicht so eindeutig, wo die entsprechenden Verarbeitungspunkte und Verantwortlichkeiten aufzufinden sind. Und in dem Maße wie das weniger deutlich und weniger klar wird, sprechen wir auch von Clouds. Wir werden über diesen etwas nebulösen Begriff heute noch Vieles hören. Ich werde das jetzt nicht vertiefen, nur so viel: Wir kennen die Cloud im Sinne einer privaten Cloud, bei der jemand IT-Ressourcen, die unter seiner Kontrolle sind, durch Virtualisierung optimal zu

nutzen versucht, also freie Kapazitäten flexibel einsetzt. Und wir kennen die öffentliche oder externe (public) Cloud, bei der IT-Ressourcen auch außerhalb des eigenen Hoheitsbereichs in ähnlicher Weise koordiniert und flexibel genutzt werden, um dadurch Effizienzvorteile durch Inanspruchnahme von gerade verfügbaren Kapazitäten zu erschließen.

Dieses so genannte Cloud Computing tritt auf verschiedenen Ebenen auf, auf der Ebene der Infrastrukturen, auf der Ebene der Plattformen und auf der Ebene der Anwendungen. Die Dienstleistungen werden als Services abgewickelt, d.h. der Leistungsnehmer braucht nicht mehr selbst die Ressourcen vorzuhalten, sondern er ruft die Leistung, die Nutzung der Ressourcen ab, wenn er sie braucht. Das gilt für Infrastruktur als Service, Plattformen als Service und Anwendungen vielfältigster Art als Service. BITKOM schätzt, dass bereits heute in Deutschland der Markt für Cloud Computing etwa 300 Mio. Euro beträgt und dass dieser Markt in den nächsten Jahren im zweistelligen Prozentbereich in der Größenordnung zwischen 30 und 50% pro Jahr wächst, überproportional übrigens bei den Anwendungen im Vergleich zur Infrastrukturnutzung in der Cloud. Dabei muss man beachten, dass solche Zahlen eigentlich nicht sehr aussagefähig sind, denn was bedeutet es, wenn 100 Mio., 50 Mio., 300 Mio. im Cloud Computing umgesetzt werden?

Wir wissen, dass die Nutzung des Cloud Computing zum Teil zu relativ geringen Preisen bei sehr hohen Volumina möglich ist, so dass diese Zahlen nicht sehr viel aussagen über das dahinter stehende Volumen. Wir wissen auch, dass nicht wenige Cloudangebote gleichsam kostenlos oder umsonst in Anspruch genommen werden. Denken Sie nur an viele Emaildienste, die in der Cloud abgewickelt werden, einschließlich der Lagerung von enormen Emailmassen, wofür der Kunde zumindest nicht unmittelbar bezahlt. Marktstudien informieren über solche riesigen Volumina in der Cloud nicht. Wir müssen davon ausgehen, dass die Cloud-Volumina, die in der Cloud als Daten und Datenverarbeitungsprozesse behandelt werden, außerordentlich umfangreich sind und exponentiell wachsen.

Unsere Konferenz möchte nun das Phänomen des Cloud Computing beleuchten. Unter welchen Bedingungen können diese doch sehr weitgehenden Arbeitsteilungen, die sich in Cloud-Strukturen abzeichnen, funktionieren? Inwieweit kann hier Vertrauen hergestellt werden als unerlässliche Voraussetzung für das nachhaltige Funktionieren dieser Märkte? Welche Anforderungen müssen private wie vor allen Dingen auch geschäftliche Kunden an das Cloud Computing richten? Welche Rechtsfragen treten auf? Welche Sicherheitsversprechen sind realistisch? Welche Regulierung ist ggf. erforderlich?

Ich bin überzeugt, dass unsere Konferenz dazu beitragen wird, diese Fragen und Zusammenhänge besser zu verstehen, auch Gestaltungshinweise zu geben und Empfehlungen an den öffentlichen und den geschäftlichen Bereich zu geben damit diese wichtige, wachsende, die Effizienz der Informations- und Kommunikations-

welt steigernde Cloud Computing nachhaltig funktionsfähig bleibt und sich für uns alle nützlich entwickelt.

Meine Damen und Herren, ich tätige diese riskante Vorleistung, dass ich darauf vertraue, dass wir solche Gegenleistungen von dieser Konferenz bekommen.

2 Trust – Herausforderungen für die IT-Versorgung heute und morgen

Uwe Bernd-Striebeck
KPMG AG, Essen

Ich habe die große Ehre, hier heute Morgen den Reigen eröffnen zu dürfen und möchte ganz kurz etwas zu meiner Person sagen. Seit 19 Jahren bin ich Partner bei der KPMG, leite da den Bereich der Technologieberatung. Das heißt, wir beschäftigen uns berufsbedingt mit den Themen, die gerade im Technologieumfeld neu am Horizont auftauchen, wobei man sich beim Thema Cloud Computing schon fragen muss, ob das wirklich alles so neu ist. Ich denke, wir starten direkt mit dem Thema. Ich habe eine ziemlich kurze und übersichtliche Agenda.

Als erster Redner heute möchte ich Ihnen kurz einige Definitionen liefern. Was ist eigentlich Cloud Computing? Was sagen andere, was Cloud Computing ist? Dann würde ich gern kurz die zurzeit am Markt verfügbaren Modelle darstellen. Was gibt es da eigentlich? Es ist durchaus beeindruckend, wenn man sieht, wer sich unter dem Begriff Cloud Computing tummelt. Dann würde ich Ihnen gern die KPMG Sicht auf die Erfolgsfaktoren darstellen und die Frage stellen, ob wir wirklich schon ein erwachsenes Business vor uns haben oder ob da noch einiges passieren muss. Nicht alles, was in der Werbung stattfindet, findet auch im realen Leben statt. Ich frage ganz kritisch: Gibt es Cloud Computing in der Form heute wirklich schon, und wo gibt es das? Als letzten Punkt würde ich Ihnen gern einen kurzen Überblick darüber geben, welche Dienstleistungen es gibt, damit es morgen dann tatsächlich ein Cloud Computing gibt.

A. Picot et al. (eds.), *Trust in IT*, DOI 10.1007/978-3-642-18110-8_2,

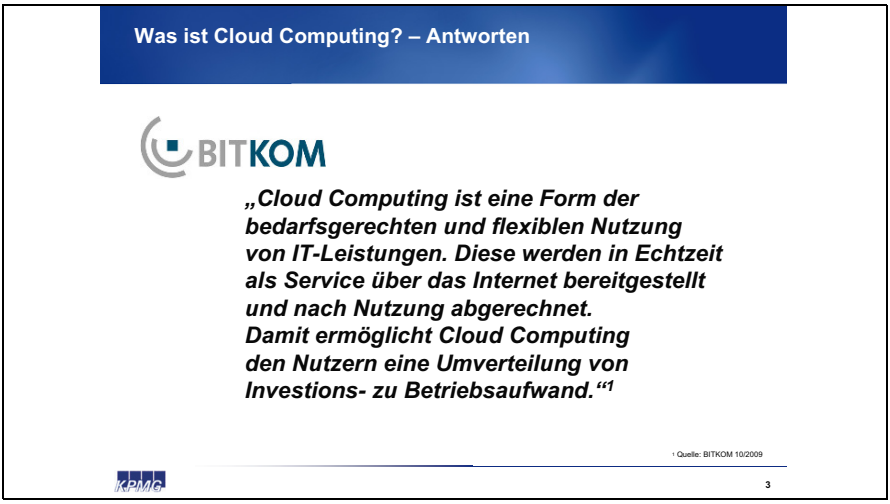


Bild 1

Ich hatte ein paar Definitionen angekündigt. Fangen wir einmal mit der von BITKOM an! Was sagt die BITKOM, was Cloud Computing ist (Bild 1). Die BITKOM hebt hervor, dass es um eine bedarfsgerechte und flexible Nutzung als Service geht. Es wird nach Nutzung abgerechnet. Das sind alles Dinge, die nicht so neu sind. Dienstleistungsrechenzentren hatten wir zum Beispiel in den 70er Jahren auch schon. Auch da war es mehr oder weniger bedarfsgerecht. Es war auch schon flexibel, und es galt schon, dass man statt eines Investitionsaufwandes eigentlich mehr einen Betriebsaufwand hatte.

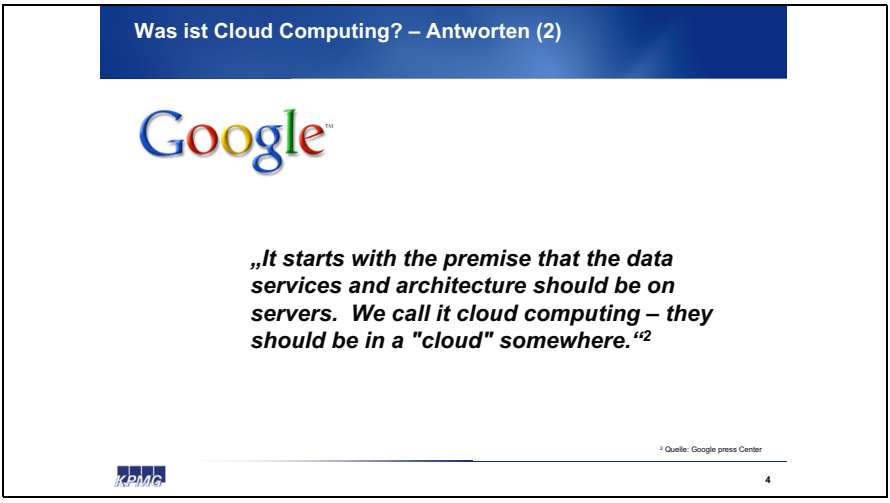


Bild 2

Eric Schmidt, der CEO von Google, hat im Jahr 2006 den schönen Spruch zum Thema Cloud Computing gesagt (Bild 2): Es beginnt mit der Voraussetzung, dass Daten auf Servern gehalten werden; wir nennen es Cloud Computing und die Daten sind irgendwo. Da haben wir schon das erste Problem. Erklären Sie das einmal Ihrem Wirtschafts- oder Ihrem Steuerprüfer, wenn der Sie fragt, wo denn Ihre Daten sind und Sie antworten, dass die irgendwo in einer Wolke sind. Ich kann Ihnen versichern, dass Sie dann das erste größere Problem haben. Dieses Problem werden wir später etwas ausführlicher beleuchten.

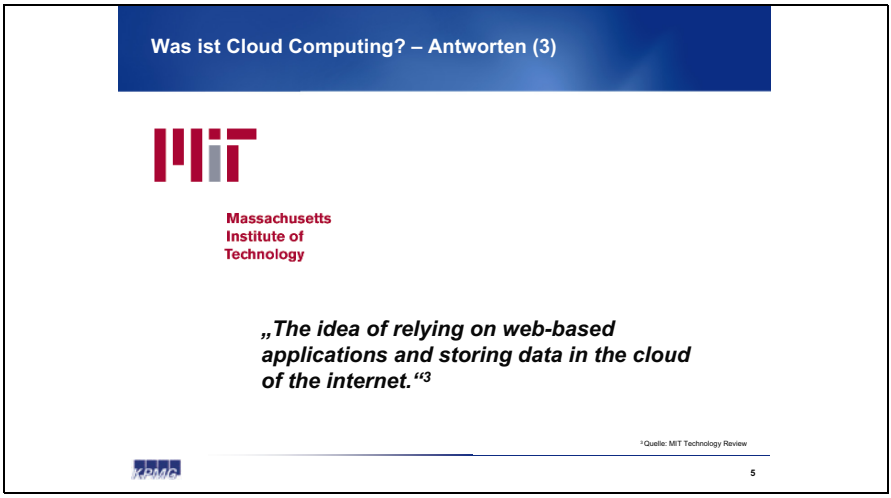


Bild 3

Eine andere interessante Idee vom Massachusetts Institute of Technology zum Thema, was Cloud Computing eigentlich ist, ist das Konzept webbasierte Anwendungen und Daten im Internet zu speichern. Das waren drei von mir ausgesuchte Interpretationen.

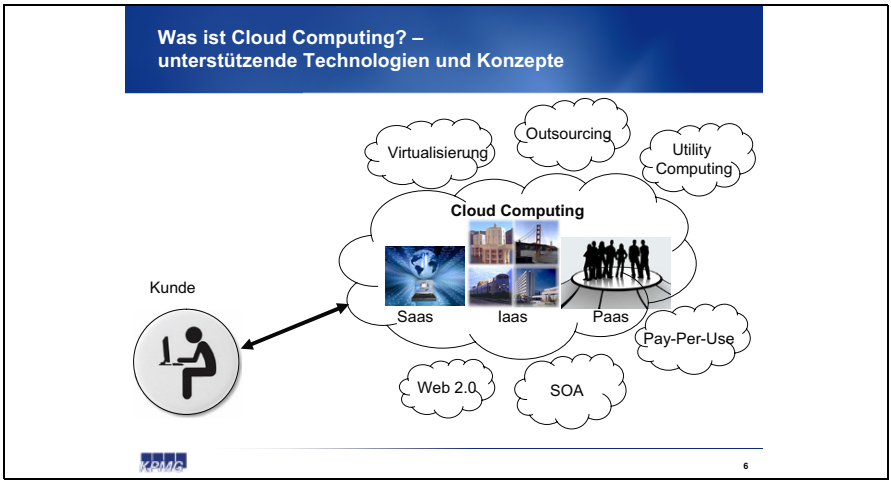


Bild 4

Wir haben keine wirklich scharfe Definition, was Cloud Computing eigentlich ist (Bild 4). Es ist sicherlich Datenverarbeitung durch fremde Dritte. Neu ist bei den meisten Komponenten, dass ich einen Zugriff über das Internet habe, was zum Beispiel aus meiner Sicht der einzige größere Unterschied zum Thema Datenverarbeitung durch fremde Dritte ist, wie wir es seit den 70er Jahren kennen. Damals hatte man eine Standleitung, die der Gesellschaft gehörte, die sie nutzte. Da war garantiert kein fremder Dritter drauf. Aber Datenverarbeitung durch fremde Dritte hatte ich damals eigentlich auch schon. Wir reden also über eine ziemlich klassische IT Dienstleistung „Datenverarbeitung durch fremde Dritte“.

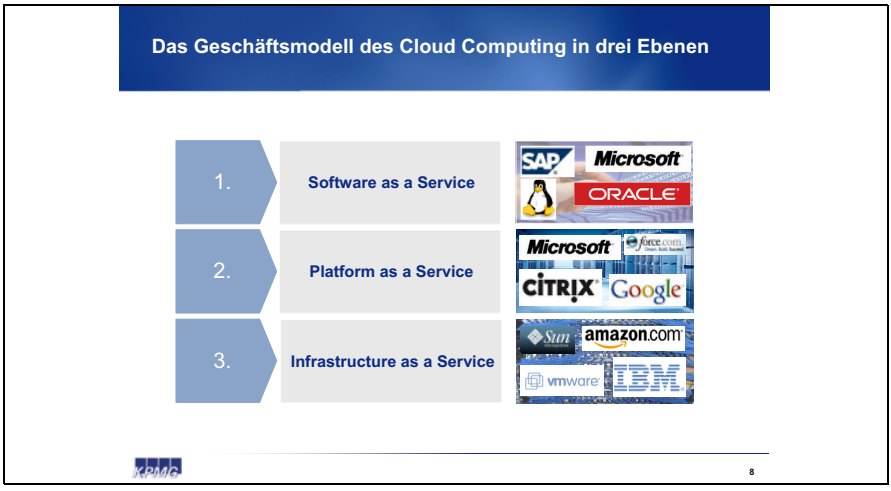


Bild 5

Im Wesentlichen haben wir heute drei Servicebereiche, Software as a Service, Infrastructure as a Service und Plattform as a Service (Bild 5). Das sind die drei Hauptgeschäftsmodelle, die man heute am Markt findet. Werfen wir einmal einen Blick darauf, was wir an Geschäftsmodellen haben. Zunächst der Bereich Software as a Service am Beispiel der SAP Software. Es ist kostenmäßig nicht ganz einfach ein SAP Kunde zu werden. Dazu bedarf es einer gewissen Unternehmensgröße und einer gewissen Unternehmenskomplexität, damit sich das lohnt. In der Vergangenheit war das so. T-Systems nennt sich selber einen der größten „SAP on Demand"-Anbieter am Markt, d.h. man kann SAP on Demand heute über das Internet beziehen. Man kann somit quasi in SAP buchen, obwohl das kostenmäßig eigentlich für die meisten Unternehmen, die sich heute so etwas leisten, früher nicht möglich gewesen wäre. Früher wäre SAP nicht in der finanziellen Schlagdistanz gewesen, kostenmäßig hätten diese Firmen wahrscheinlich niemals über SAP nachgedacht sondern vielmehr über KHK Software.

Da ist zu erkennen, welchen Kundentypus wir da eigentlich vor uns haben. Da reden wir durchaus von einem anderen Kunden von der Größe und von der Marktpositionierung her, als wir das bisher klassischerweise im SAP Umfeld hatten. Wenn man einen ersten Blick darauf wirft, wer sich da tummelt, was man an Software kaufen kann, sind das durchaus alles bekannte Namen und Logos. Ähnlich ist es bei Plattform as a Service, wo auch die üblichen Marktführer unterwegs sind. Es taucht kurioserweise so ein Name wie Google auf. Wie kommt Google da eigentlich hin?

Wir kennen alle die Suchmaschine, und eigentlich kennt man Google nur daher. Ich hatte neulich das Vergnügen auf einer anderen Konferenz über Cloud Computing einen Vertreter von Google dazu zu hören. Google hat aufgrund dieses Browsers, den wir alle kennen und aufgrund der dahinterliegenden Technologie so viel Hardware einkaufen müssen, dass die sehr gute Preise bekamen, was ihnen heute ermöglicht, selber als Plattformanbieter aufzutreten. Das ist zum Beispiel die Geschichte, die dahinter steckt, warum Google heute als Plattformanbietet auftritt.

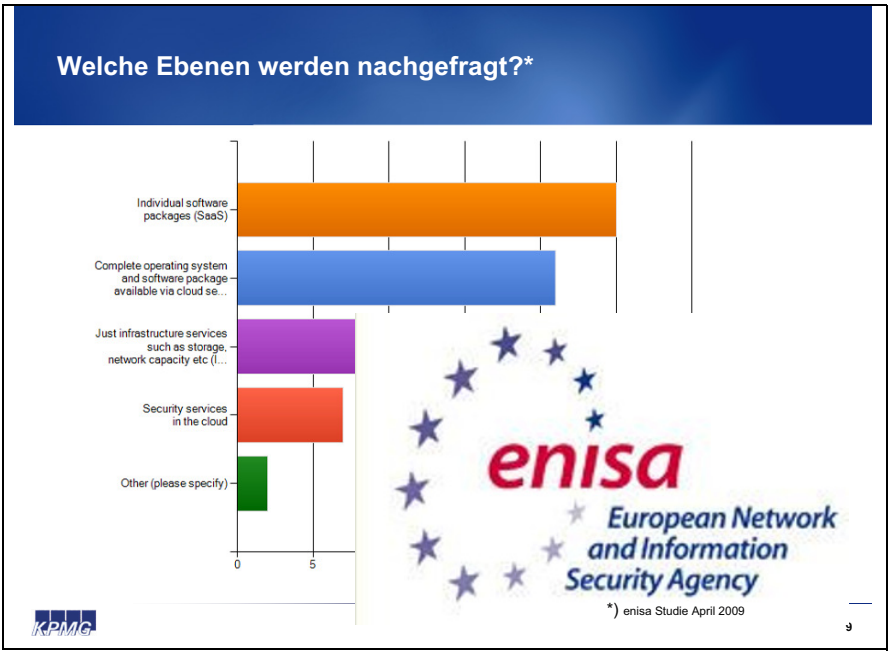


Bild 6

Im Bereich Infrastructure haben wir auch die üblichen Marktteilnehmer wie IBM, EDS usw.

Was fragt der Markt eigentlich nach? Darüber gibt es eine interessante Studie von der ENISA European Network, einer Information Security Agency (Bild 6). Es wurden Kunden befragt, welche Ebenen tatsächlich nachgefragt werden. Dabei ist herausgekommen, dass die größte Nachfrage nach Software as a Service Dienstleistungen besteht. Danach kam Plattform as a Service, der blaue Balken, und als Drittes wurden Infrastrukturdienstleistungen nachgefragt. Fast auf Augenhöhe damit war der Wunsch nach Security Dienstleistungen. Wenn Sie jetzt an meine Worte von eben denken, welchen typischen Kunden wir da eigentlich haben und wir uns ein Schwergewicht aus dem DAX nehmen, ob das ein Thyssen Krupp, Siemens, Daimler oder wer auch immer ist, so ist für die Security kein Thema, was man outsourcen würde. Das heißt, wenn ich also eine starke Nachfrage nach Security Dienstleistungen bekomme, rede ich über ein ganz anderes Kundenumfeld und auch über eine andere Art von Dienstleistungen als wir das bisher bei Datenverarbeitung durch fremde Dritte hatten.

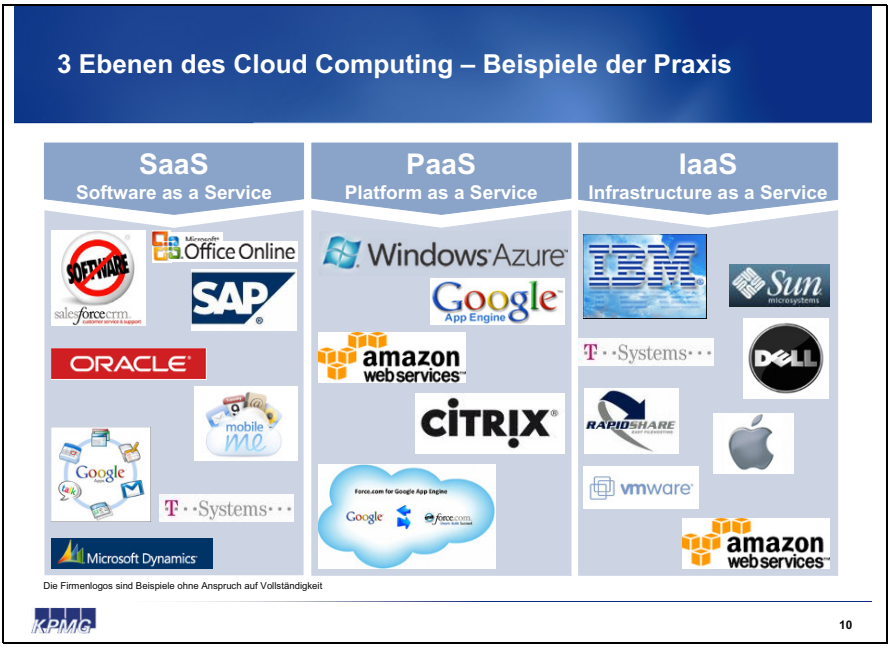


Bild 7

Werfen wir einen Blick in die Praxis von Software as a Service! Ich sprach es eben schon an, SAP on Demand (Bild 7). Ich kann heute ein Microsoft Office im Internet quasi on Demand nutzen, indem ich es nicht mehr auf einen Rechner ziehe, d.h. ich habe im Prinzip kein Word mehr auf dem Rechner, sondern schreibe da nur noch meine Briefe. Ich glaube, an der Stelle ist es sehr hilfreich, wenn sich jeder selbst die Frage stellt. Ich finde es praktisch, wenn ich nicht Word kaufen müsste für private Dinge. Es kostet eine Menge Geld und in Wirklichkeit schreibt man vielleicht zwei Briefe im Monat. Trotzdem stelle ich mir die Frage, ob ich Word nutzen und meine Briefe vielleicht auch im Internet speichern würde? Gehen Sie einmal in sich und denken darüber nach, welche Briefe man schreibt. Vielleicht korrespondiert man mit einem Arzt oder mit einem Mieter oder vielleicht mit einem Scheidungsanwalt, wenn man gerade Pech hat. Das sind alles Dinge, von denen ich nicht möchte, dass die plötzlich im Internet stehen. Da haben wir alle ein großes Fragezeichen im Kopf, ob diese Dinge da wirklich in guter Hand sind.

Dasselbe trifft eigentlich auch auf diese Google Apps zu, die quasi eine Art Outlookersatz sind. Ich möchte auch nicht, dass alle Welt Zugriff auf meinen Terminkalender hätte. Wir haben da ziemlich viele Angebote, auch durchaus erwachsene Angebote. Salesforce bietet zum Beispiel eine CRM Lösung an. Das sind alles schon Angebote, die auch den Businesskunden durchaus im Blick haben. Die Frage ist immer: trauen wir uns?

Bei Plattform as a Service, wie ich eben schon sagte, sind einige neue Player aufgetaucht. Google aus den eben schon genannten Gründen. Bei Amazon sieht es ähnlich aus. Auch die hatten durch jahrelanges Einkaufen von Infrastruktur plötzlich so gute Preise, dass sich diese Möglichkeit geboten hat.

Bei Infrastructure as a Service gibt es eigentlich nichts wirklich Neues, wenn man das in Vergleich zu den 70er Jahren stellt. Auch damals bot IBM schon Dienstleistungen an. Der einzige Unterschied, den ich heute feststellen kann, ist die Zugriffsart, wobei man sich fragen muss, wie viel Zugriff bei Infrastructure as a Service tatsächlich über das Web stattfindet. Da würde ich ein großes Fragezeichen vermerken. Man sieht bei Infrastructure as a Service, dass auch solche Namen wie Rapidshare auftauchen, die eigentlich in einer völlig anderen Liga spielen als eine IBM. Rapidshare ist ein Dienst, wo man Daten im Internet austauschen kann und was vorwiegend zum Verteilen von MP3s oder Filmen benutzt wird, mit Sicherheit keine Businessanwendung.

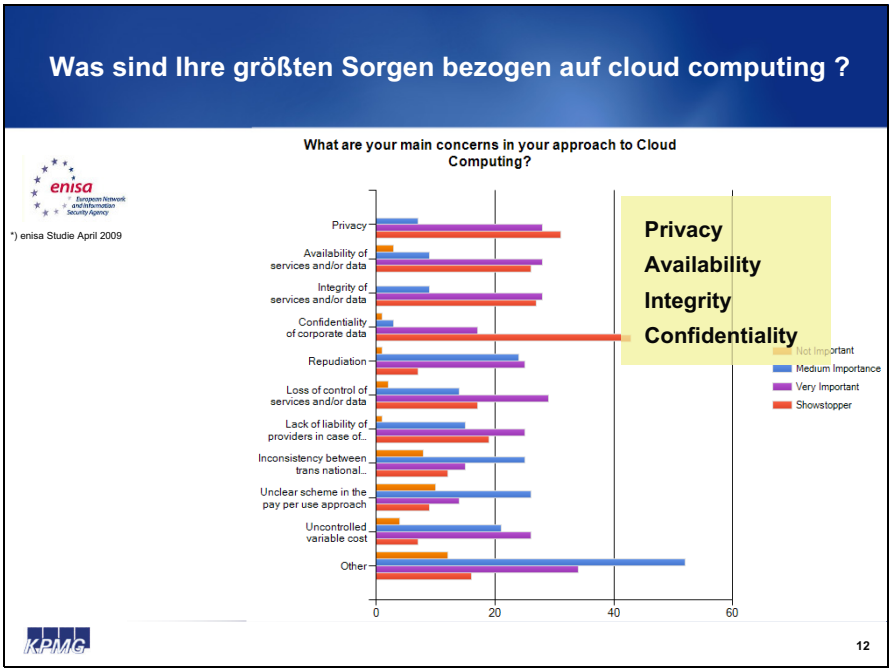


Bild 8

Kommen wir zu dem Erfolgsfaktor Trust und was die potentiellen Kunden eigentlich denken. Auch dazu hat die ENISA Umfrage aus dem Jahr 2009 einige sehr interessante Erkenntnisse geliefert (Bild 8). Auf der rechten Seite sehen Sie die Klassifizierung der Antworten. Das helle Orange bedeutet nicht wichtig, Blau war mittlere

Wichtigkeit, Lila sehr wichtig und das Orange unten sind Showstopper. Wo sind diese am längsten? Das ist oben bei dem Thema Privacy, also Datenschutz. Bei dem Thema Availability ist der Showstopperbalken ziemlich lang. Bei dem Thema Confidentiality of Corporate Data ist er unheimlich lang, wie bei Vertraulichkeit und bei Integrity. Offenbar sind das die Dinge, die den Anwender wirklich interessieren; Datenschutzverfügbarkeit, Integrität und Vertraulichkeit von Daten. Wenn man dieser Studie Glauben schenken darf, sind das die Schlüssel zum Erfolg.

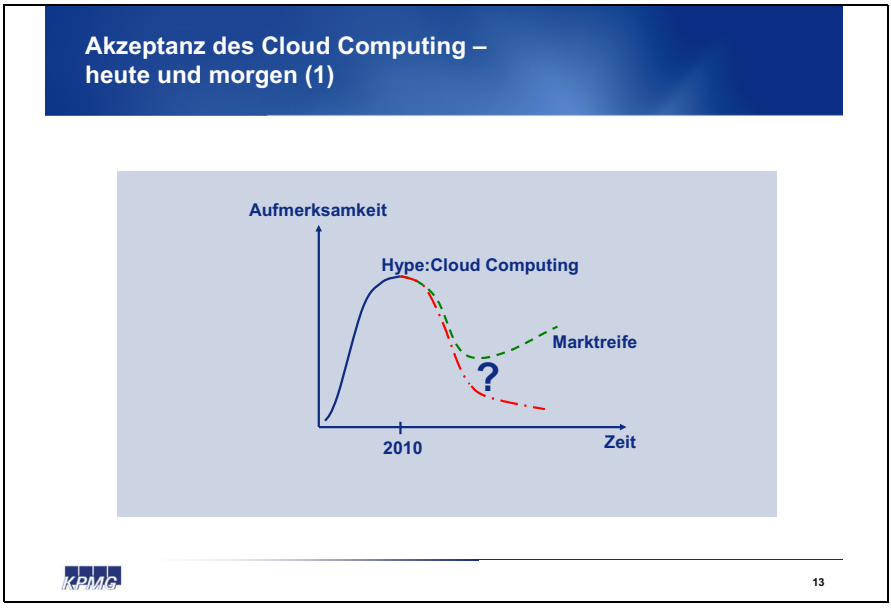


Bild 9

Wie sieht es mit der Akzeptanz am Markt aus? Im Augenblick haben wir einen absoluten Hype (Bild 9). Alle sprechen über Cloud Computing. Wie geht es weiter? Cloud Computing ist in aller Munde. Meine These ist, dass Cloud Computing eigentlich heute nicht wirklich erwachsen ist. Ich werde das gleich mit einigen Beispielen untermauern. In der nächsten Zeit wird es sich entscheiden, ob die Produkte, die wir heute sehen, wirklich eine Marktreife haben. Werden wir da einen Wachstumstrend sehen? Wenn die aber nicht endlich erwachsen werden und auf einen höheren Reifegrad kommen, den wir eigentlich beim klassischen Dienstleistungsbereich im IT- Dienstleistungsbereich heute haben, glaube ich, dass in vier oder fünf Jahren von diesem Begriff Cloud Computing keiner mehr spricht. Die Frage ist auch, wann wir Erfolg haben.

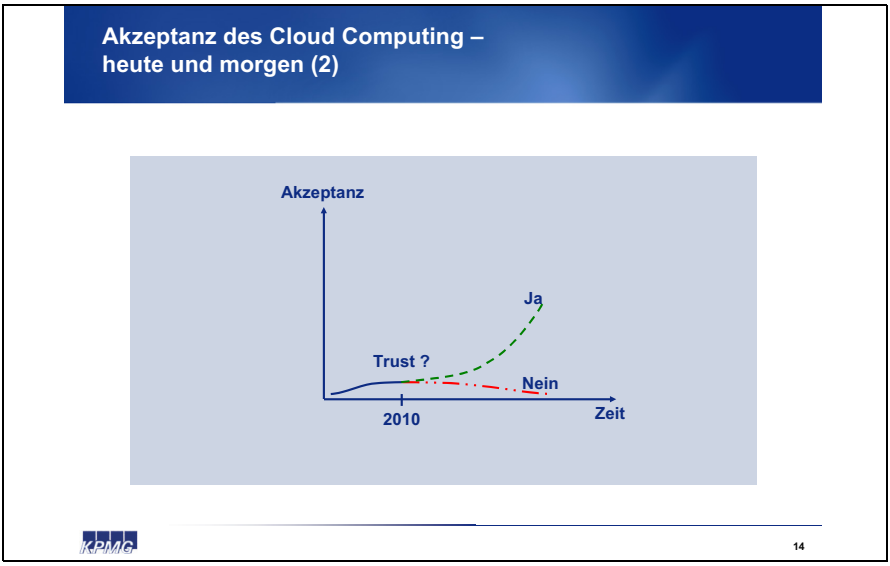


Bild 10

Wir sind im Moment an der Stelle, dass wir uns wie zum Beispiel heute bei dieser Konferenz fragen, ob wir eigentlich Trust haben (Bild 10). Und wenn wir Vertrauen haben, dann wird die Kurve hochgehen und wenn wir das nicht haben, wird das Thema letztlich in der Bedeutungslosigkeit verschwinden. Da bin ich ziemlich sicher.

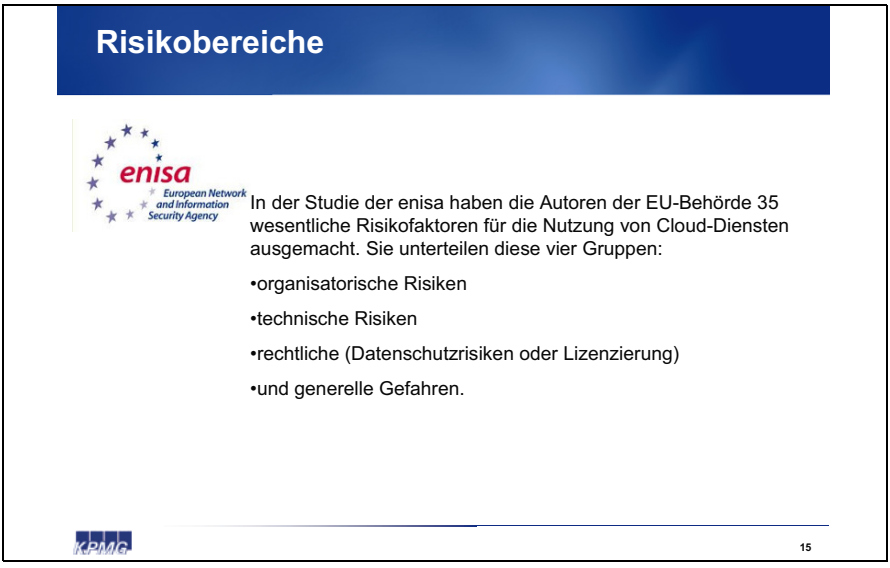


Bild 11

Was sind die Risikobereiche? Die von mir bereits mehrmals zitierte Studie unterteilt die Risikobereiche in vier Gruppen (Bild 11). Es gibt organisatorische, technische, rechtliche und generelle Risiken, was eigentlich nichts Neues ist. Ich glaube auch nicht, dass wir Herausforderungen haben, die uns vor ganz neue Dinge stellen. Ich glaube vielmehr, dass wir einfach die üblichen Dinge, die schon immer auch mit der Sorgfaltspflicht eines ordentlichen Kaufmanns zu tun hatten, anwenden müssen, und zwar auch auf die Angebote von Cloud Computing.

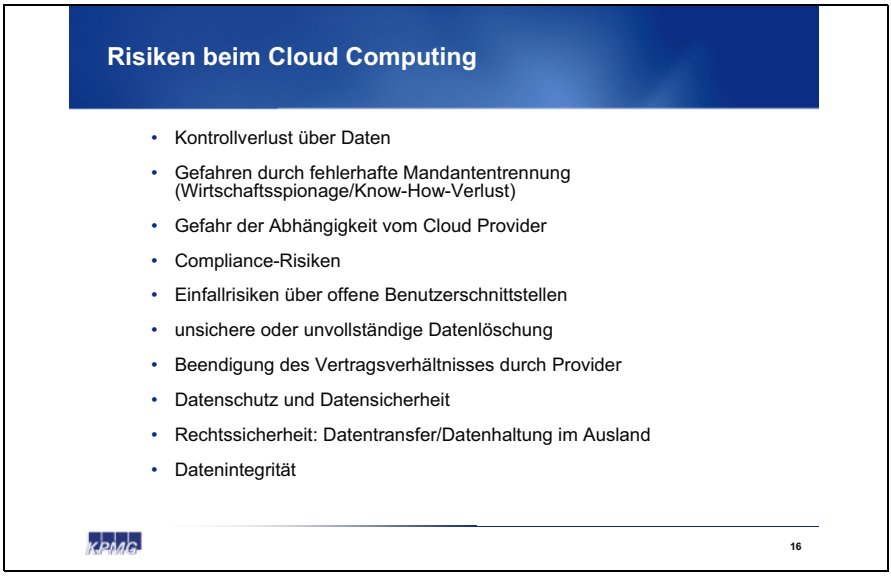


Bild 12

Was in diesen Umfragen immer wieder genannt wird, ist ein Kontrollverlust über Daten, d.h. dass man die selber nicht mehr im direkten Zugriff hat (Bild 12). Was macht man, wenn der Anbieter den Vertrag kündigt? Ein typisches SAP Beispiel: Ich miete mir einen Buchungskreis oder natürlichen Mandanten innerhalb eines SAP Systems. Welche Art von Mandantentrennung habe ich eigentlich? Alle, die mit SAP Systemen umgehen, wissen, dass es sehr wohl Transaktionen, Tabelleneinstellungen gibt, die Mandanten übergreifend gelten. Auf all diese Dinge habe ich in Wirklichkeit keinen direkten Zugriff. Ich weiß es nicht. Ich kaufe einen Mandanten, in dem ich buchen kann. Ich glaube, dass vielen Kunden heute diese Risiken gar nicht bewusst sind, weil sie aus einer anderen Liga kommen.

Ich zitiere gern noch einmal die Schwergewichte aus dem DAX. Die würden niemals einen SAP on Demand kaufen, weil in dieser Liga die Risiken, die sich aus einer Mandantentrennung im SAP ergeben können, durchaus bekannte Themen sind. Natürlich habe ich eine starke Abhängigkeit von dem Cloud Provider, denn eine solche Umstellung ist mit hohen Kosten verbunden. Wenn der mir morgen

meinen Vertrag kündigen kann, habe ich möglicherweise diese Kosten ein weiteres Mal.

Ich möchte noch einmal auf den Kontrollverlust eingehen. Das geht einher mit Compliance Risiken, denn man muss sich bei allem, was man tut, darüber im Klaren sein, dass man selbst der Buchführungspflichtige und auch der Steuerpflichtige ist. Genauso wie Sie heute haftbar gemacht werden können, wenn Ihr Steuerberater irgendwelche Dinge nicht richtig macht, sind Sie dem Finanzamt gegenüber erst einmal in der Haftung. Bei Unternehmen ist das natürlich auch so. Sie müssen als Gesellschafter die Compliance-Anforderungen einhalten. Wenn Sie das aber outsourcen, dann muss man sehr viel Sorgfalt walten lassen, damit man das trotzdem im Griff hat. Werfen Sie einmal einen Blick auf Ihre SLAs. Sind darin Prüfungsrechte für Ihren Wirtschaftprüfer, für die Betriebsprüfer vereinbart? Ist da wirklich klar geregelt, welche Kontrollen der Provider übernehmen soll? Das haben wir heute selbst im IT Dienstleistungssektor nicht. Natürlich gibt es Kontrollen in diesem Bereich, die auch ziemlich stereotyp abgearbeitet werden. Aber was ist, wenn eine Regel außer Kraft gesetzt wird? Ich will Ihnen kurz etwas aus der Praxis erzählen. Wenn wir heute Ordnungsmäßigkeitsprüfungen machen, wissen die Größten in der Branche natürlich alle, wie man ein Dienstleistungsrechenzentrum fährt. Eine der Grundregeln aus Sicherheitssicht ist, dass ich natürlich meine Server auf einem einheitlichen Patchlevel halte. Trotzdem finden wir bei jeder Prüfung in den Serverfarmen irgendwelche Server, die nicht auf dem gleichen Patchlevel sind. Das liegt nicht etwa daran, dass die dort arbeitenden Leute nicht wissen, was sie tun. Nein, es sind die Kunden selbst, die anrufen und ihr Quartalsreporting brauchen und wollen, dass ihr Server am Wochenende nicht runtergefahren wird. Dann nutzen all die zertifizierten Kontrollen gar nichts mehr. Das sind die Fälle, wo in der Praxis dann tatsächlich die Schwierigkeiten auftauchen.

Unvollständige Datenlöschung ist ein anderes Thema, für das ich noch ein tolles Beispiel habe. Jeder, der heute oder gestern die Zeitung aufgeschlagen hat, weiß, dass das ein ganz großes Thema ist. Gerade für den Zugriff auf Kundendaten haben wir viele Beispiele von CDs von großen Kommunikationsgesellschaften. Die Zeitungen sind voll mit solchen Fällen und ganz ehrlich, Kundendaten haben wir alle. Auch da muss man sich sehr genau überlegen, was man tut, wenn man solche Dinge outsourct.

Wie sieht es mit der Datenhaltung im Ausland aus? Neulich auf einer Konferenz sagte mir einer der anderen Referenten aus dem Board von Rapidshare: wir Deutschen sind immer die Bedenkenträger, es ist doch völlig egal, wo der Server steht. Mein alter Professor sagte immer: ein Blick ins Gesetz erleichtert die Rechtfindung, und da steht leider drin, dass es eben nicht egal ist, wo der Rechner steht, sondern er muss im Verfügungsbereich der EU stehen als Minimum und nicht in einer Cloud oder irgendwo. Das geht leider nicht.

Ich habe Ihnen noch ein Beispiel aus dem Leben mitgebracht. Es gibt bei HP und allen anderen Großen auch ein Produkt wie Flexible Computing. Da kann man sich

Großrechnerkapazitäten mieten, um irgendwelche aufwändigen Berechnungen durchzuführen. In der Bankenlandschaft gibt es so etwas wie eine Monte Carlo Simulation. Dabei werden die kompletten Portfoliodaten, nachdem die Kundendaten abgeschnitten wurden, auf den Rechner geschoben. Das wird Monte Carlo Simulation genannt, weil man quasi wie beim Würfeln simuliert, was eigentlich passiert, wenn der Ölpreis steigt oder fällt, was ein steigender oder fallender Dollar macht. Damit berechnet eine Bank im Prinzip, wie viel Spielraum sie noch hat und wie gut oder schlecht sie mit ihrem Portfolio aufgestellt ist. Das ist so ziemlich der heilige Gral einer jeden Bank, weil, wenn eine Bank diese Portfoliozusammensetzung von einer anderen Bank wüsste, könnten sie die bei bestimmten Geschäften gezielt unterbieten oder überbieten, weil man genau weiß, wie viel Spielraum der andere noch hat. Das ist von der Vertraulichkeit her ein ziemlich sensibles Thema, und dieses Produkt Flexible Computing schreit eigentlich geradezu danach, weil so etwas bei einer Bank drei-, viermal vorkommt und ansonsten steht das Blech im Keller herum und wird nicht benutzt. Sie brauchen dafür so viele Rechnerkapazitäten, dass sich das absolut lohnen würde.

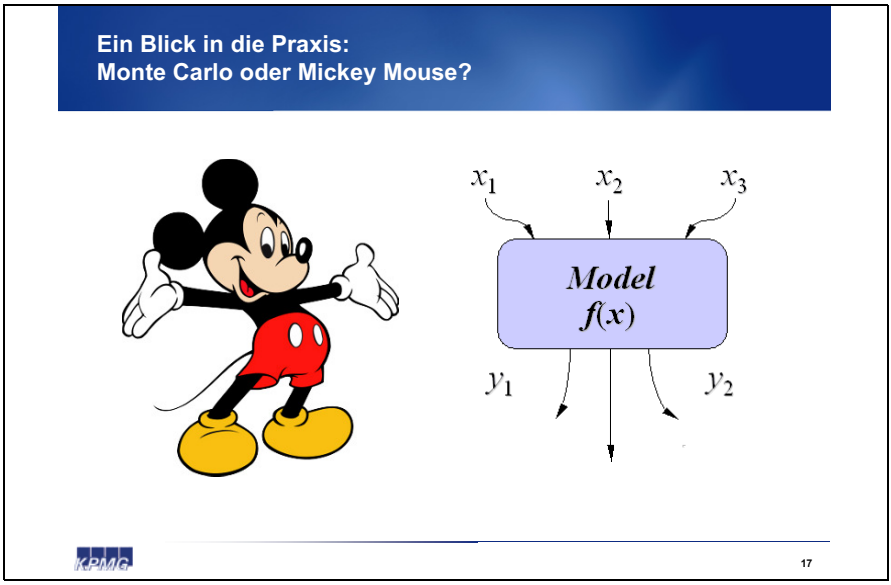


Bild 13

In der Realität fragt man sich aber, wer so etwas kauft. Mieten die Deutsche oder Dresdner Bank so etwas? Nein. Die haben eigene Hardware im Keller stehen obwohl sie sie nur drei- oder viermal pro Jahr brauchen. Wer aber sehr wohl diese Rechnerkapazitäten nutzt, ist zum Beispiel Walt Disney zum Rendern von neuen Mickey Mouse Filmen (Bild 13). Die nutzen das, spielen ihre Daten auf, rendern den Film, ziehen die Daten wieder ab – alles wunderbar.

Woran liegt das? Beim Mickey Mouse Film ist es egal, wenn ein Teil der Informationen wegkommt. Bei der Deutschen Bank ist es nicht egal, wenn Portfoliodaten wegkommen. Die haben einfach kein Vertrauen in den Datentransfer, in die Verarbeitung schon. Die Frage ist aber zum Beispiel auch, wie sicher diese Festplatten hinterher gelöscht werden. Oder kann die Mickey Mouse vielleicht doch noch Portfoliodaten sehen, wenn sie als nächster auf diesen Rechner kommen? Dieses Beispiel zeigt, wo heute die Grenzen sind für eine Nutzung von solchen Diensten. In dem Augenblick, wo wir ernsthafte Daten haben, wo wir wichtige Businessdaten haben, wo ich einen hohen Anspruch an Vertraulichkeit habe, findet aus meiner Sicht nur sehr marginal ein Geschäft statt. Es gibt viele Bereiche, wo die Vertraulichkeit der Daten einen anderen Stellenwert hat. Mickey Mouse Daten; da findet sehr wohl ein Geschäft statt. Wenn man sich das heute von der Verteilung her anguckt, wo tatsächliche schon richtig messbares Geschäft in Euro läuft, werden Sie genau diese Aufteilung wiederfinden.

Bild 14

Die Presse streut im Augenblick auch ziemliche Skepsis in diese Studie und sagt: Vertrauen ist gut, Kontrolle ist besser (Bild 14). Der Blätterwald rauscht auch in diese Richtung. Es sind alles tolle Angebote. Es ist ein gutes Geschäftsmodell, mit dem man ordentlich Geld sparen könnte. Aber können wir es eigentlich machen?

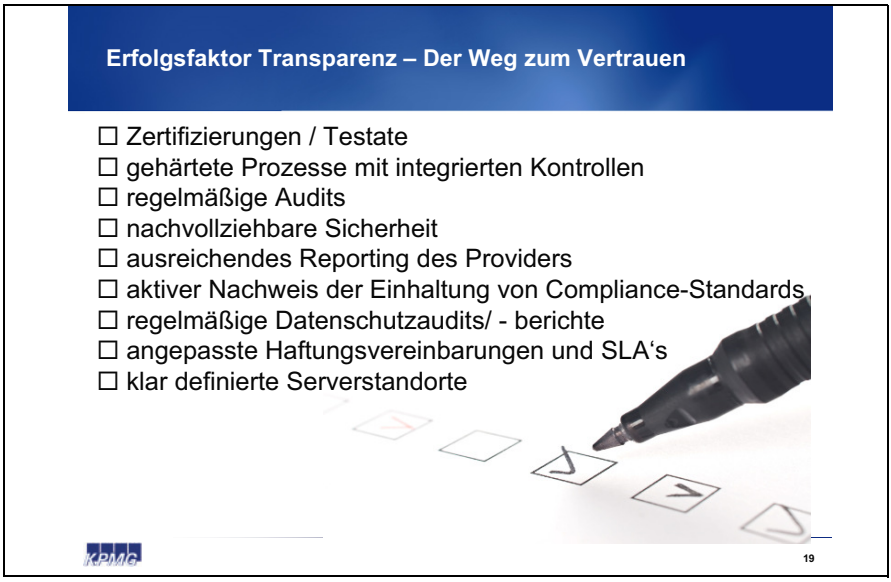


Bild 15

Ich habe hier ein paar Punkte ausgearbeitet (Bild 15). Wann würde dieses Geschäftsmodell wirklich zum Tragen kommen? Wann würden auch große Firmen und ernstzunehmende Businesskunden auf diesen Zug aufspringen? Ich glaube, es gibt ein paar Dinge, aber Sie werden nichts Neues finden. Ich habe eben schon gesagt, dass wir einfach die vorhandenen Dinge auf Cloud Computing vernünftig anwenden.

Das geht erst einmal los, dass wir Zertifizierungen oder Testate brauchen. Vielleicht brauchen wir auch da einen neuen Standard. Wir verdienen selber auch unser Geld mit diesen SAS 70 Zertifizierungen. Die erfüllen auch ihren Zweck, wobei man da jetzt sagen muss, dass ich zur Absicherung der kaufmännischen Sorgfaltspflicht natürlich auf einem anderen Level bin, als wenn ich mich vor Hackern schützen will. Das ist von der Qualität her schon noch einmal etwas anderes. Ich glaube, wir haben da heute keinen wirklichen Standard, den man nutzen kann. Wir können auch nur nach den Standards prüfen, die es heute gibt, und da fehlt uns eigentlich noch was. Man muss, wenn man so etwas einführt, vernünftig auf die Härte der Prozesse achten. Man muss vernünftige integrierte Kontrollen haben. Ich glaube, für einen Dienstleister gehört es sich auch, dass er regelmäßige Audits machen lässt, denn viele behaupten vor den Kunden, dass sie vom Namen her vertrauenswürdig sind. Ich hätte da in Teilen meine Zweifel. Die Sicherheit, die wir haben, muss nachvollziehbar werden. Dazu gehört auch, dass man mehr Offenheit von der Providerseite bekommt, dass es vielleicht ein Reporting gibt und nicht nur immer heile Welt sondern auch, welche Regelverstöße man hat. Jeder, der sich einmal mit dem Verfassungsschutz unterhalten hat, weiß, dass regelmäßige Statistiken gemacht werden,

wie viel Angriffe zum Beispiel auf bestimmte Domänen stattfinden. Warum bietet ein großer Dienstleister nicht solche Dinge an und sagt, wir sind im Moment einem größeren Druck von außen ausgesetzt, tun aber etwas dagegen? Das würde alles mehr Transparenz schaffen. Oft fehlt mir auch ein aktiver Nachweis der Einleitung von Compliance Standards. Ich will keinem zu nahe treten. Die Kontrollen werden durchgeführt. Die Frage ist immer, was ist, wenn ich die eben von mir dargestellte Ausnahme, ein Overrouling durch das Management stattfindet.

Die meisten Haftungsvereinbarungen und SLA‘s sind ausgesprochen lückenhaft im Hinblick auf Cloud Computing. Da wird nicht wirklich geregelt, wer eigentlich welche Kontrollen macht und wer eigentlich wann in der Verantwortung steht. Wenn ich eine Geschäftsleitung habe, brauche ich klar definierte Serverstandorte. Da kann es nicht dem Provider freistehen, ob der Rechner auf den Philippinen oder sonst wo steht. Das geht nicht.

Bild 16

Was bieten wir für Dienstleistungen an? Zu den meisten Dingen kann in der Tat die KPMG etwas beitragen (Bild 16). Wir bieten Zertifizierungen und Testate an, natürlich unter den eben genannten Einschränkungen und nur nach den Standards, die der Markt heute hergibt. Wir bieten Security von Anwendungen und vor allem von Prozessen an. Wir beraten auch gern bei einer Einführung und helfen bei einer Anbieterauswahl. Wir kennen uns gut mit Verträgen und SLA’s aus. Die technischen Dinge, die Sie für Ihr Tagesgeschäft brauchen, haben Sie als Gesellschaft in der

Regel gut im Griff. Es geht eigentlich um die Dinge, die nicht Tagesgeschäft sind, dass man da Prüfungsrechte vereinbart, dass man einen Nachweis von Kontrollen, die der Provider hat, entsprechend hat. Dass man ein intelligentes Reporting über solche Dinge mit aufnimmt. Da sind wir schon bei Ordnungsmäßigkeitsprüfungen. Und in der Regel habe ich noch eine ganze Reihe an steuerlichen und datenschutzrechtlichen Fragestellungen, gerade wenn so ein Server aus deutscher Sicht die deutschen Grenzen verlässt. Bitte sprechen Sie mich bei Bedarf gerne direkt an.

3 Anforderungen eines Unternehmens der Energiewirtschaft an vertrauenswürdige ITK

Dr. P. Unkel und Dr. W. Puritz
RWE Power AG

Einführung

Thema des Vortrages sind die Anforderungen eines Unternehmens der Energiewirtschaft an vertrauenswürdige Informations- und Kommunikations-Technik, aufgezeigt am Beispiel der RWE Power AG, der deutschen Stromerzeugungsgesellschaft des RWE Konzerns.

Die Anforderungen an einen Stromerzeuger sind hoch und sehr spezifisch ausgeprägt. Davon ausgehend werden die Anforderungen an ITK sowie die im Verlaufe der IT-Entwicklung der letzten Jahrzehnte immer wieder veränderten IT-Lösungen diskutiert und vergleichend der Entwicklung des Strommarktes gegenüber gestellt. Schließlich wird die aktuelle Neuerung: Cloud-Computing in diesem Zusammenhang thematisiert.

Die Anforderungen des Unternehmens

Die Anforderungen an ITK sind eng verknüpft mit der Geschäftstätigkeit. RWE Power ist einer der großen Stromerzeuger in Europa. Rund ein Drittel der in Deutschland verbrauchten Strommenge wird in Kraftwerken der RWE Power erzeugt. Die Stromerzeugung erfolgt dabei in einem Energiemix aus Kernenergie, fossilen Energieträgern wie Steinkohle, Gas und Braunkohle sowie aus Wasserkraft. Daneben gibt es innerhalb des Konzerns weitere Gesellschaften, die Geschäftsfelder eines Energieversorgers abdecken, wobei laufende Optimierungen immer wieder zu Veränderungen führen. So wurde z.B. in 2008 die RWE Innogy gegründet, die die Stromerzeugung europaweit aus regenerativen Energiequellen ausbaut. In 2009 wurde z.B. die bisherige RWE Energy umgebildet und ganz aktuell, seit 01.01.2010, ist die neu gegründete Gesellschaft RWE Technology konzernübergreifend verantwortlich für alle Kraftwerksneubauten.

Die Hauptgeschäftsprozesse der RWE Power sind einerseits die Stromerzeugung aus den verschiedenen Energieträgern sowie die Gewinnung von Braunkohle in den Tagebauen des Rheinischen Braunkohlereviers (Bild 1). Diese Geschäftsprozesse bedingen den Einsatz komplexer Großanlagen, die jeweils im Industrievergleich über sehr lange Zeiträume genutzt werden und deshalb immer wieder Wartungs-,

A. Picot et al. (eds.), *Trust in IT*, DOI 10.1007/978-3-642-18110-8_3,

Instandhaltungs- und auch Modernisierungsmaßnahmen unterliegen. Ein Beispiel hierfür sind die Großgeräte der Tagebauförderung, die zu den größten beweglichen industriellen Maschinen weltweit gehören. Diese Großanlagen sind – vor dem Hintergrund der rationellen großtechnischen Gewinnung und Erzeugung – in hohem Maße von Automatisierung und Prozessleittechnik geprägt. Diese Orientierung auf Langfristigkeit und Stabilität mit der Zielsetzung hoher Versorgungssicherheit des Strommarktes bedingt stabile und nachhaltig optimierte Geschäftsprozesse. Betrieb und Instandhaltung sowie deren laufende Optimierung haben hohen Stellenwert; dies findet beispielsweise Ausdruck in den speziell ausgebildeten Betriebs- und Instandhaltungsprozessen mit entsprechender IT-Unterstützung.

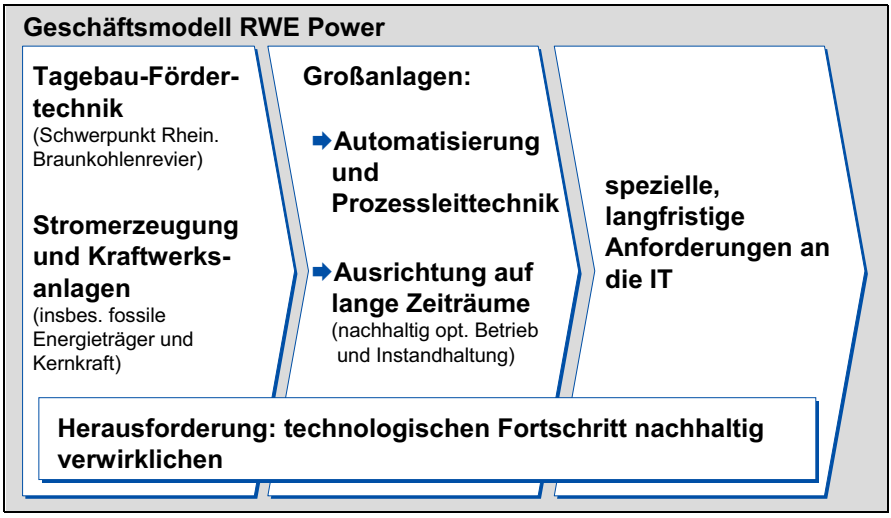


Bild 1: Von Großanlagen geprägte Geschäftsprozesse bei RWE Power

Zur Erhaltung und zum Ausbau der Wettbewerbsfähigkeit ist die laufende Verbesserung der Energieerzeugung, der Braunkohlenförderung und generell der Unternehmensprozesse eine ständige Herausforderung. Energieforschung wie im Bereich neuer Kraftwerkstechniken zum Beispiel zur Wirkungsgradsteigerung und zur CO_2-Verminderung/ -Vermeidung mittels Carbon-Capture-and-Storage(CCS) und Integrated-Gasification-Combined-Cycle(IGCC) haben hohen Stellenwert. Auch im Braunkohlentagebau wird die kontinuierliche Verbesserung stark forciert. Insgesamt liegt besonderes Augenmerk darauf, technologischen Fortschritt nachhaltig zu verwirklichen – diesem Anspruch muss auch die IT entsprechen.

Das Spektrum der IT-Unterstützung bei RWE Power (Bild 2) reicht vom Einsatz marktgängiger Lösungen über spezielle, kernprozessspezifisch ausgerichtete IT bis zur Prozessdatenverarbeitung und Prozessleittechnik mit sehr hohem technischen Verfügbarkeits- und Sicherheitsanspruch. In querschnittsorientiert angelegten Pro-

zessen können vorwiegend marktgängige IT-Anwendungen eingesetzt werden (z.B. Lösungen zu Enterprise Resource Planning). Je mehr sich diese Prozesse an weit verbreiteten Standards orientieren, wie sie in vielen Unternehmen zur Anwendung kommen, desto mehr kann man die zugehörigen IT-Lösungen als IT-Commodities ansehen. Im Bereich kernprozessspezifisch ausgerichteter IT ist die Situation geprägt von am Markt bezogenen, aber stark angepassten IT-Systemen und von Eigenentwicklungen. Insbesondere im Braunkohlentagebau sind kaum IT-Lösungen am Markt verfügbar; Eigenentwicklungen also häufig die einzige Möglichkeit. Den Kern-Prozessen und ihrer IT-Unterstützung kommt generell wettbewerbsdifferenzierende Bedeutung zu. Daher befinden wir uns hier in einem sehr unternehmensspezifisch ausgeprägten Umfeld. Im Fokus einer übergreifenden Steuerung der IT und ihrer Systeme steht eine ganzheitliche Prozessunterstützung, die einen integrativen Einsatz der verschiedenen IT-Systeme erfordert.

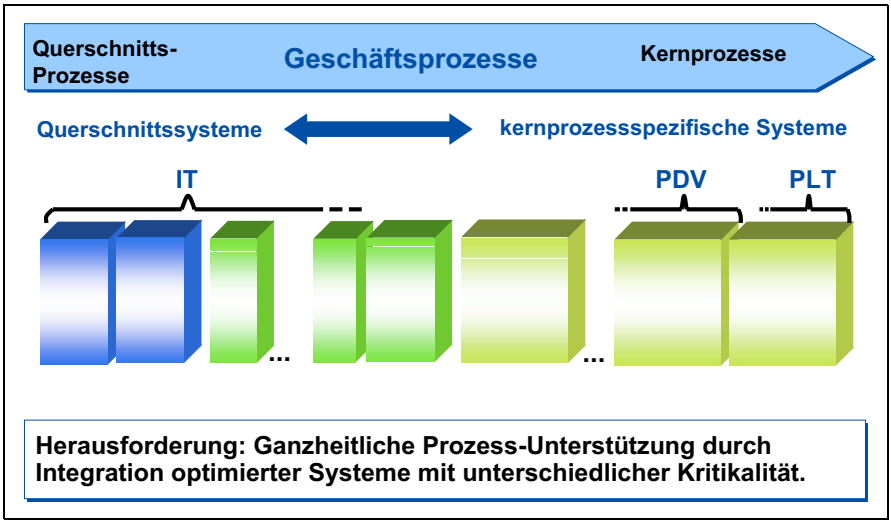


Bild 2: Spektrum der IT-Unterstützung der Prozesse bei RWE Power

Die Anforderungen des Anwenders

Die Erwartungshaltung der Anwender ist heute in hohem Maße von ihrer IT-Nutzung, vor allem auch im privaten Bereich, geprägt (Bild 3). Großer Einfluss kommt hier naturgemäß aus der Internet-Nutzung; die User Interfaces und Funktionalitäten des Internet-Browsers sowie Inhalt und Funktion des dortigen Angebotes prägen die Anwendererwartungen und Nutzungsgewohnheiten. Auch die IT in Unternehmen muss diesen Anforderungen mit einer entsprechenden Darstellung der Inhalte und erwartungsgemäßem „Look and Feel“ folgen, um IT-Anwendern eine motivierende und ansprechende IT-Umgebung zur Unterstützung ihrer Aufgaben im Unternehmen und im Prozess zu bieten.

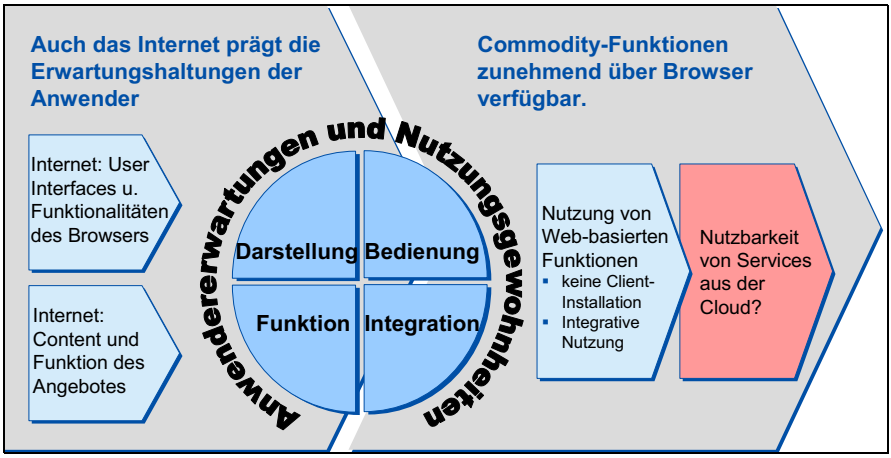


Bild 3: IT-Nutzenerwartungen am Arbeitsplatz

Die im Internet zunehmend verfügbaren Commodity-Funktionen halten Einzug sowohl in die private als auch in die Arbeitsplatz-IT-Nutzung. Hierzu zählen Funktionen wie Suchmaschinen, Wikipedia, Routenplaner und Ähnliches, deren Nutzung heute wie selbstverständlich im Rahmen unserer Informationsversorgung zur Gewohnheit wird. Der Betrieb solcher Services erfolgt aus Sicht des Internet-Nutzers vielfach in der Cloud, das heißt, Erwartungsumfang und Leistungsinhalt der Services sind klar umrissen, über Aspekte des Betriebs (Betreiber, Ort des Rechenzentrums, Wartung etc.) besteht hingegen nur geringe oder keine Kenntnis. Die Nutzungsart und -intensität ist meist erfahrungsgeprägt. Das heißt, solche Serviceangebote werden dann genutzt, wenn es gute Erfahrungen mit Verfügbarkeit, Inhalt etc. gibt. Festzustellen ist auch, dass der Nutzungskontext dieser Informationen dazu führt, dass die Verfügbarkeit nicht besonders kritisch ist. Die genutzten Services stellen vom Inhalt her oftmals ergänzende Funktionen dar oder sind als Commodity in ausreichender Redundanz verfügbar, so dass der Nutzer auf die Verfügbarkeit im Einzelfall meist weniger stark angewiesen ist.

Die jederzeitige Verfügbarkeit, an jedem Ort (Connectivity vorausgesetzt) sowie leichte Ansprechbarkeit und standardisierte Inhalte (Bild 4) führen dazu, dass der Internetnutzer sich um den Betrieb und seine örtliche Zuordnung keine Gedanken macht, und daraus auch eine Erwartungshaltung an den betrieblichen IT-Alltag bildet. In einem betrieblichen Kontext kann durch am Markt verfügbare Standards die günstige Situation entstehen, dass eine früher für eine Aufgabe speziell entwickelte IT-Funktion durch eine inzwischen im Internet verfügbare Commodity-Funktion abgelöst werden kann. Z.B. hat die Entwicklung der heute standardisierten, weit verbreiteten Mobilfunktechnologie dazu geführt, dass zumindest ein Teil der früher erforderlichen speziellen Betriebsfunktechniken abgelöst werden konnte.

Mit zunehmend höherem Entwicklungsstand der IT wird dem Benutzer eine Entkopplung von der technischen Komplexität ermöglicht. Die Nutzung der umfangreichen, komplexen Technologie wird durch verbesserte oder standardisierte Bedienung, Komponenten und Schnittstellen(Kapselung), die sich durchsetzen, zunehmend vereinfacht. Oftmals bedeutet dies, dass eine intuitive Bedienung ermöglicht wird.

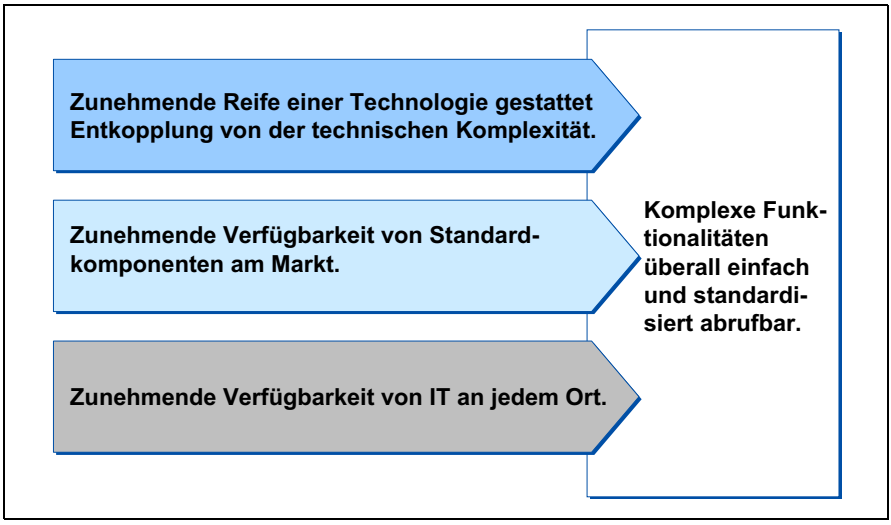


Bild 4: Erwartungen des IT-Anwenders

Außerhalb der IT ist die Entwicklung des Automobils hierfür ein Beispiel. In der Frühzeit des benzinmotorgetriebenen Fahrzeugs musste der Fahrer sich um Aspekte wie manuelle Zündungsverstellung, Ankurbeln des Motors von Hand oder unsynchronisierte Gangwechsel kümmern und die Bedienung war noch dazu oftmals sehr fahrzeugspezifisch ausgeprägt. Heutige Automobile hingegen bieten eine weitgehend normierte und vor allem einfache, komfortable Bedienung trotz erheblich gesteigerter Funktionalität. Vergleicht man die Entwicklung in der IT, so stellt man rasch fest, dass einerseits im heutigen Stand immer noch eine hohe Weiterentwicklungsdynamik zu beobachten ist, sich andererseits aber zugleich auch hier Normierungen etc. der Bedienung zunehmend herausbilden. Informations- und Serviceangebote im Internet lassen sich ohne besondere Schulung, also intuitiv, nutzen, und Grundfunktionalitäten präsentieren sich verstärkt in ähnlicher Weise. Mit der technischen Weiterentwicklung formt sich die Erwartungshaltung des Anwenders, und speziell in der IT wird sie naturgemäß stark durch das überall verfügbare Internet geprägt. Vor allem wird das Handeln des Anwenders zunehmend vom „Denken in IT-Kategorien“ befreit: An die Stelle einer technikorientierten Sichtweise tritt eine Konzentration auf die fachliche Aufgabe. Mit einfacher, leicht verständlicher Bedienbarkeit und hoher Verfügbarkeit stellen sich meist auch Kosteneffekte ein – das

(IT-)Werkzeug wird kosteneffizienter und ermöglicht eine kostengünstige Durchführung des Geschäftsprozesses. Es ergibt sich eine Erhöhung des Wertbeitrages des Geschäftsprozesses.

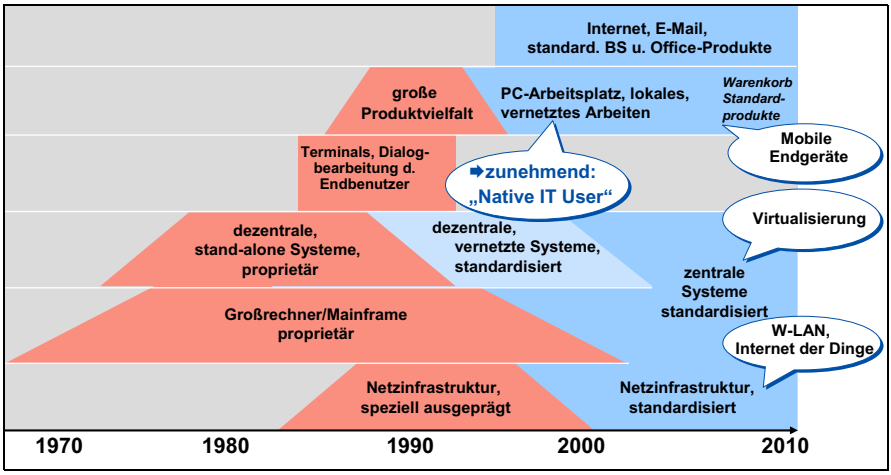


Bild 5: IT-Markt: hohe Entwicklungsdynamik noch immer ungebrochen – IT-Entwicklung bei RWE Power

IT-Entwicklung bei RWE Power

Als relativ junge Technologie weist die IT auch heute noch, wie bereits erwähnt, eine hohe Entwicklungsdynamik auf (Bild 5). Bei RWE Power wurden ab Ende der siebziger Jahre mit PC, mittlerer Datentechnik und Prozess-Rechnern neben der zentralen IT auch dezentrale IT-Strukturen geschaffen: IT-Lösungen konnten jetzt direkt vor Ort in den lokalen Geschäftsprozess am jeweiligen Standort integriert werden. Diese Entwicklung hat eine Dualität von zentraler und dezentraler IT entstehen lassen, die im Lauf der IT-Entwicklung immer wieder mit unterschiedlichen Schwerpunkten diskutiert wurde, aber auch neue Möglichkeiten für verteilte Systeme bot. Im Vergleich zu dem hier genannten ersten Trend zur Dezentralisierung ist mit dem heute diskutierten Cloud-Computing ein Trend in Richtung Zentralisierung verbunden. Der Ära des Großrechners folgten die unternehmensweiten Client-Server-Architekturen auf Basis weit verbreiteter Hardware- und Software-Systeme und relationaler Datenbanktechnik. Parallel dazu entwickelten sich Möglichkeiten zum flächendeckenden Einsatz von ERP-Standardsoftware im Großunternehmen. Die Benutzungsoberflächen entwickelten sich von der reinen Batch-Verarbeitung über die Dialogverarbeitung zur grafischen Benutzeroberfläche, die wir in ihren verschiedenen Ausprägungsformen spätestens seit den neunziger Jahren gewohnt sind. In der weiteren Entwicklung wird der Schritt zur intuitiven, „natürlichen“ Oberfläche (NUI) erwartet, die die bereits erwähnte intuitive, realitätsnahe Bedienung ermöglicht. Auch bei der Analyse der IT-Anforderungen hat sich einiges ver-

ändert. Heute steht der Geschäftsprozess im Vordergrund. Für RWE Power ist die strukturierte Prozessdokumentation bereits seit Mitte der neunziger Jahre ein unverzichtbares Mittel der Weiterentwicklung der Prozesse und ihrer IT-Unterstützung. Dem liegt die Erkenntnis zugrunde, dass eine Betrachtung der IT und der Prozesse, die sie unterstützt, nicht voneinander getrennt werden kann. Stichworte der weiteren Entwicklung sind der zunehmende Einsatz mobiler Endgeräte, Virtualisierung und Wireless LAN sowie das „Internet der Dinge“, ermöglicht durch die Nutzung der Radio-Frequency-Identification(RFID)-Technologie. Auf Seiten der IT-Nutzer kann man inzwischen von so genannten „native IT Usern“ sprechen: Vertreter einer jüngeren Generation, die bereits von Anfang an mit IT groß geworden sind und für die die Nutzung von IT in weitaus größerem Maße selbstverständlich ist. Rückkopplungseffekte aus der Erwartung dieser IT-Nutzer an die Struktur der IT-Anwendungslandschaft sind zwangsläufig und liefern neue und wertvolle Impulse der Weiterentwicklung.

Insgesamt haben in dem betrachteten Zeitraum die ITK-Anwender viele z.T. gravierende Veränderungen miterlebt. Immer wieder waren Chancen und Risiken des Neuen abzuwägen und Vertrauen in Neues aufzubauen.

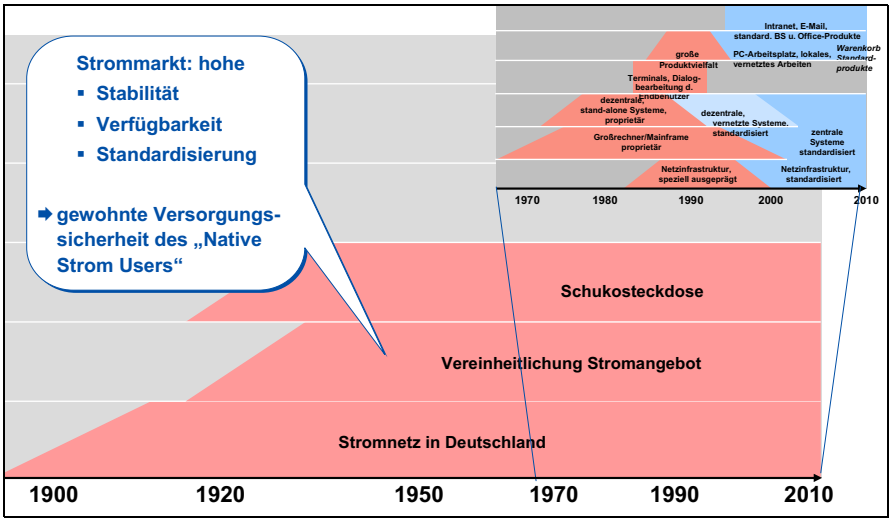


Bild 6: Strommarkt: Nutzungsgewohnheiten und -erfahrungen

Vergleich der Entwicklungen von IT und Energiewirtschaft

Im Betrachtungskontext der RWE Power ist es, gerade vor dem in der IT diskutierten Vergleich zur Energiewirtschaft (z.B. Nicholas Carr: THE BIG SWITCH, NY2008) mit Formulierungen wie: „IT wie Strom aus der Steckdose“ interessant, für die IT-Entwicklung Parallelen zur Entwicklung des Strommarktes zu disku-

tieren (Bild 6). Die Entwicklungsgeschichte der Stromversorgung ist deutlich älter als die der IT und beginnt Anfang des 20. Jahrhunderts. Das erste RWE Kraftwerk ging 1900 in Essen in Betrieb, das erste Braunkohlenkraftwerk war 1915 das Goldenberg-Werk in Hürth bei Köln. Die theoretischen Grundlagen der Elektrizität sind mit den Maxwell-Gleichungen ab etwa 1860 gelegt worden. Es folgten eine Reihe von Erfindungen wie z.B. der Wechselstromgenerator und der Transformator Ende des 19.Jahrhunderts. Die Theorie ging damals dem Praxiseinsatz zeitlich deutlich voraus.

Seit langer Zeit ist also der Strombezieher vom Strommarkt ein hohes Maß an Stabilität, Verfügbarkeit und auch Standardisierung – symbolisiert durch die Schutzkontakt-(Schuko-)-Steckdose – gewohnt. Wir alle sind also seit langem „Native Strom User“ mit einer genau so ausgeprägten Erwartungshaltung, und verlassen uns in sehr vielen Bereichen des täglichen Lebens ganz selbstverständlich auf die Verfügbarkeit von Strom.

Demgegenüber ist die IT-Entwicklung nach wie vor geprägt von einer ungebrochenen Dynamik; die grundsätzlichen IT-Architekturen unterliegen auch heute noch einem Wandel. Bei RWE Power ist seit den siebziger Jahren eine Entwicklung auf der Ebene der IT-Anwendungsarchitektur zu beobachten, die ressourcenbedingt bei monolithischen Systemen begann, weiter zur strukturierten Programmierung und anschließend zur Objekt-Orientierung führte. In jüngerer Vergangenheit werden die Client-Server-Architekturen zunehmend durch webbasierte Anwendungen ergänzt bzw. abgelöst, und die weitere Entwicklung wird vermehrt Service-Orientierte-Architekturen(SOA) und Web-Services bringen.

In der Dynamik der Weiterentwicklung der IT ist Cloud-Computing als eines der nächsten Themen derzeit in der Diskussion. Neben vielen anderen, relevanten Aspekten, auf die auch im Rahmen dieser Veranstaltung eingegangen wird, setzt die Nutzung von Services aus der Cloud nach Einschätzung der Autoren die serviceorientierte Architektur (SOA) bzw. die Nutzung von Web-Services als Architekturmerkmal voraus. Die Basis für die integrierte Nutzung wird eine reife IT-Landschaft bzw. IT-Prozessunterstützung sein, die sich durch gute Integration (Interoperabilität interner und externer Komponenten) auszeichnet.

Architekturbetrachtung

Vor diesem Hintergrund macht ein eher abstrakter Blick auf die Architekturentwicklung Sinn (Bild 7). Die IT-Entwicklung, insbesondere auch die bei RWE Power, war immer schon von der Suche nach der optimalen Struktur geprägt. Im Laufe des Weges hat es einige Paradigmenwechsel gegeben. Getrieben wurde die Entwicklung von Faktoren wie Kostenreduzierung, Ressourcenoptimierung, Risikominderung und Beherrschung der Komplexität. Ausdruck fand die Weiterent-

wicklung in der Suche nach der optimalen Struktur und dem damit einhergehenden Wandel der Strukturen. Hiermit verbundene Zielstellungen sind Erhöhung der Flexibilität und Sicherheit sowie Nutzung von Standards. Geschäfts- und Kostenanforderungen zielen auf Wartbarkeit, Nachhaltigkeit und auch die Wiederverwendbarkeit von Elementen der Struktur.

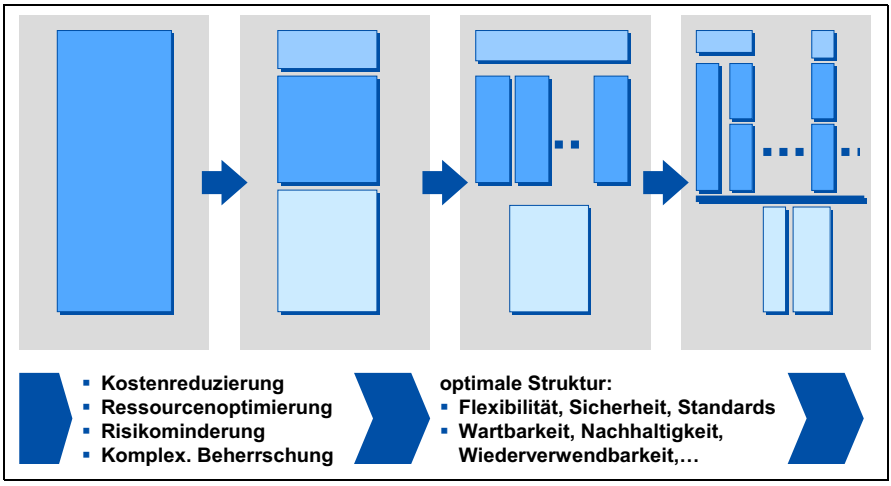


Bild 7: Die Suche nach der optimalen Struktur – Weiterentwicklung der IT-Architekturen zur Erfüllung der Anforderungen

Eine grundsätzlich in der Ausbildung und Weiterentwicklung von Strukturen zu beobachtende Tendenz ist eine zunehmende, skalierbare Granularisierung, die die vorgenannten Optimierungsziele aufgrund vermehrter Flexibilität und Adaptierbarkeit für spezielle Fachprozessanforderungen unterstützt. Deutlich wird dies beispielsweise an der Anwendungsarchitektur, die zunehmend den Schritt von großen monolithischen Anwendungssystemen, die speziell auf gegebene Fachprozesse zugeschnitten sind und diese damit auch relativ fixiert abbilden, hin zu kompakteren, aber auch flexibler nutzbaren Funktionseinheiten bzw. Services vollzieht. Hier dargestellt sind neben der monolithischen Form die 3-Schichten-Architektur (Benutzungsoberfläche-Anwendungsschicht-Datenhaltung), die bei zunehmender funktionaler Erweiterung durch mehrere Module die gemeinsame Datenhaltung auch zur Integration einsetzt und die Service-Orientierte-Architektur(SOA), die neben Anwendungen, speziellen und gemeinsam genutzten (shared-) Services auch einen Integrationsrahmen (Enterprise Service Bus) umfasst.

Die Suche nach der „optimalen“ Struktur findet sich nicht nur in der IT. Wer in ein Radio der fünfziger Jahre hineinschaut wird die monolithische Struktur erkennen mit einer Grundplatine auf der die Röhren und alle übrigen elektrischen Bauelemente montiert sind. Ein Blick in einen heute typischen Tower-PC zeigt eher das

SOA-Bild: Man kann Funktionen in Form genormter Platinen mit Standardschnittstellen in den bestehenden Integrationsrahmen einstecken und das Bus-System sorgt für das integrierte Zusammenwirken aller Funktionen. Es gibt auch Analogien zu shared services wie z.B. das Netzteil und die Klimatisierung.

Spezielle Anforderungen RWE Power

An Stromversorger werden, insbesondere weil sie auch Teil der kritischen Infrastrukur eines Landes darstellen, hohe Erwartungen bezüglich Sicherheit und Verfügbarkeit gestellt (Bild 8). Dies ergibt sich auch aus bestehenden Verpflichtungen der Stromlieferverträge und vor allem auch aus den erfahrungsgeprägten Erwartungen der Kunden und der gesellschaftlichen Verantwortung des Unternehmens.

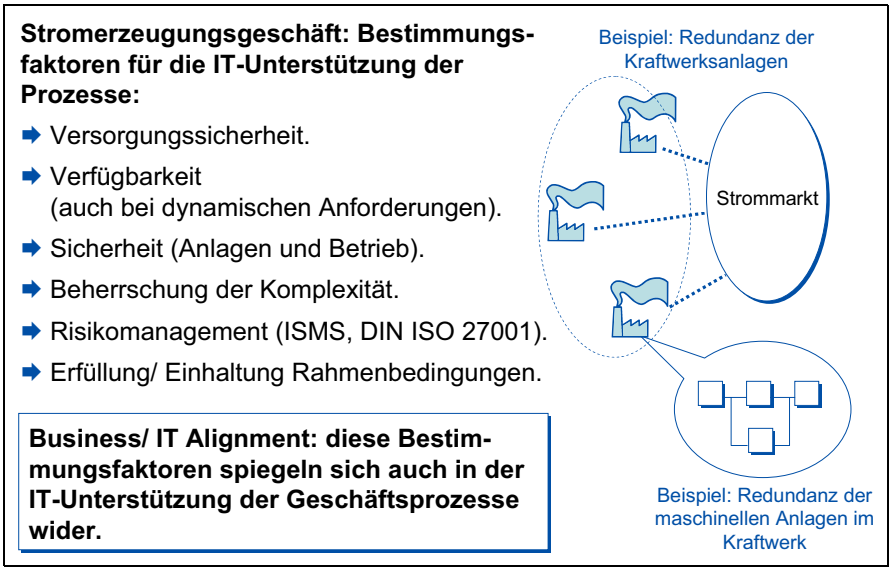


Bild 8: Spezielle Geschäftsanforderungen, insbesondere Sicherheit und Risikomanagement

Hieraus leiten sich die entsprechenden Bestimmungsfaktoren für die IT-Unterstützung der Prozesse ab, die die Geschäftsziele bezüglich Versorgungssicherheit, Verfügbarkeit – auch bei dynamischen Anforderungen (z.B. je nachdem wie der Strom aus Windkraftanlagen entsprechend der Wettergegebenheiten zur Verfügung steht) –, Sicherheit der Anlagen und des Betriebs, Beherrschung der Komplexität, Risikomanagement und Erfüllung von Rahmenbedingungen unterstützen müssen. Stellvertretend soll an dieser Stelle eine typische Möglichkeit für die Umsetzung der Anforderungen mit Hilfe von Redundanz zur Erfüllung der Geschäftsziele beschrieben werden. Redundanz schaffen ist ein wichtiger Aspekt des betrieblichen Planungs- und Dispositionsprozesses und gilt für alle Ressourcen wie Anlagen,

Ersatzteile etc. Mittels Prozessanalyse werden die kritischen Abhängigkeiten erkannt und analysiert. Dabei ist auch darauf zu achten, scheinbare Redundanzen zu erkennen und zu vermeiden, die zum Beispiel dann entstehen, wenn der Ausfall einer verdeckten, gemeinsamen Funktion oder Ressource eine Nutzung redundant vorgehaltener Kapazitäten unmöglich macht. Beispiel: Telekommunikation per Festnetz-TK-Anlage und per Mobilfunk erscheinen auf den ersten Blick redundant. Es kann aber durchaus sein, dass in einer räumlich begrenzten Umgebung beides mit der gleichen Stromversorgung betrieben wird, was die Redundanz auflöst.

Anforderungen dieser Art sind, wie alle Anforderungen, Bestandteil des nachhaltigen Business/ IT Alignments bei RWE Power (Bild 9). Die Bestimmungsfaktoren der Geschäftsprozesse müssen sich in der Ausgestaltung der IT-Unterstützung widerspiegeln. Das Verständnis von Business/ IT Alignment ist das eines komplexen Zusammenwirkens aus Geschäftsprozess und IT im Hinblick auf ein optimiertes Gesamtergebnis. Ein gutes Business/IT Alignment ergibt sich nicht von allein sondern muss aktiv gefördert werden. Bei RWE Power wirkt hier primär die Fachabteilung „Informationsmanagement“ auf ein gutes Zusammenwirken an der Schnittstelle zwischen Fachprozess und IT ein.

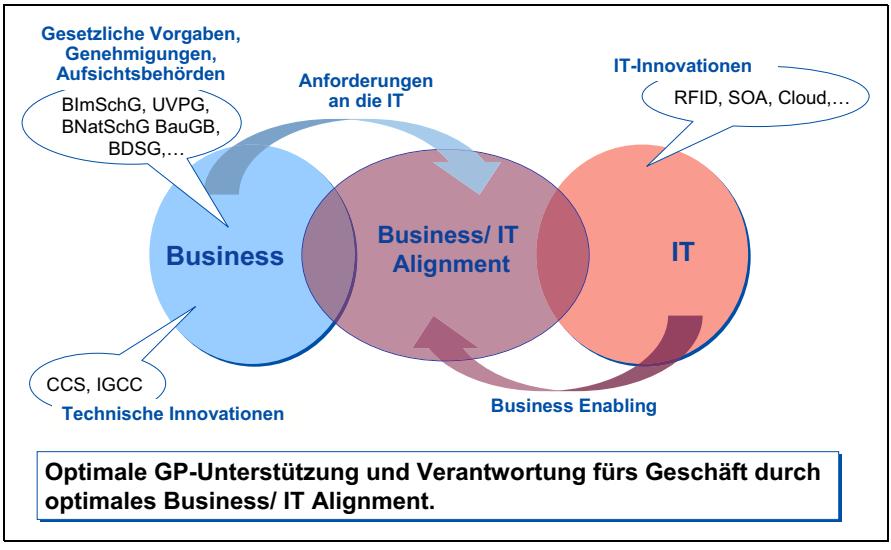


Bild 9: Business-/ IT-Alignment, beispielhafte Anforderungen an Geschäftsprozesse und damit an die IT

Als Bestimmungsfaktoren fließen in die Anforderungen des Geschäftsprozesses an seine IT-Unterstützung beispielsweise gesetzliche Anforderungen bzw. Auflagen ein, die es zu beachten gilt. Im Gewinnungsprozess der Braunkohle und in der Stromerzeugung gibt es eine große Zahl relevanter gesetzlicher Bestimmungen, wie

z.B. das Energiewirtschaftsgesetz, das Bundesnaturschutzgesetz, das Bundesimmissionsschutzgesetz und vieles mehr.

Technische Weiterentwicklungen oder auch Innovationen, die im Geschäftsprozesskontext, am Markt oder in Forschung und Entwicklung erkennbar sind, finden ebenfalls Eingang in die Abläufe des Geschäftsprozesses und seine IT-Anforderungen. Ein gutes Zusammenspiel von Business und IT bezieht auch Weiterentwicklungsimpulse aus „Business Enabling durch IT“ ein – gemeint ist hiermit eine Befähigung des Geschäftsprozesses mittels IT. Von besonderem Interesse sind vor allem Neuerungen vom IT-Markt (IT-Innovationen) in Anwendung auf die spezielle IT-Unterstützung der Geschäftsprozesse. Hierzu haben in der Vergangenheit z.B. SOA und RFID gezählt, aktuell sind hier z.B. die Impulse des Cloud-Computing zu betrachten. Voraussetzung der Ausübung einer solchen „enabling“-Funktion ist eine profunde Kenntnis aller Geschäftsprozesse des Unternehmens, der IT-Entwicklungen am Markt, ein gutes Vertrauensverhältnis und Kenntnis von fachlichen Ansprechpartnern, aber auch eine offene Atmosphäre im Unternehmen, die die Einbringung konstruktiver Ideen fördert. Bei RWE Power werden IT-Innovationen insbesondere in den systematisch und regelmäßig durchgeführten Fachstrategiegesprächen thematisiert.

Fazit

Zusammenfassend ergibt sich, dass Einsatz und Weiterentwicklung der Unternehmens-IT abhängt von einer Vielzahl von Bestimmungsfaktoren aus dem IT-Umfeld (Bild 10). Hierbei kann man unterscheiden zwischen: Generellen Vorgaben, Beteiligten, Rahmenbedingungen und Leistungszielen der IT.

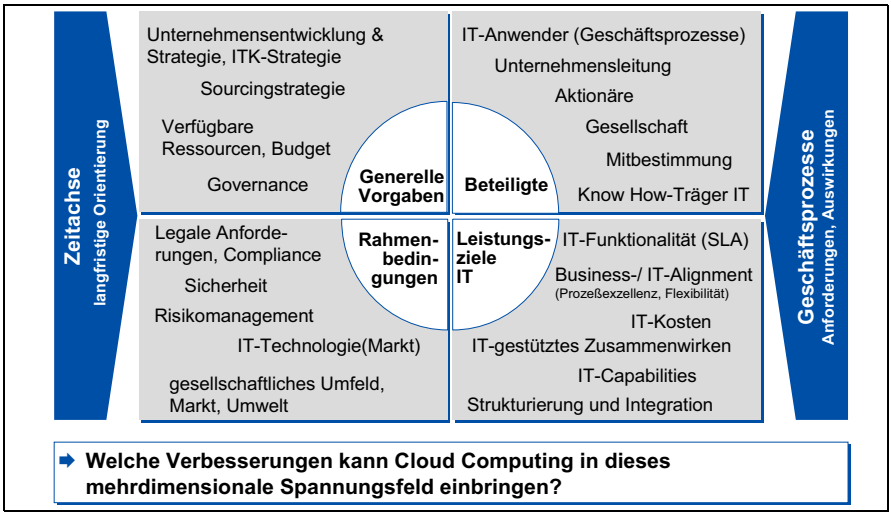


Bild 10: Bestimmungs- und Einflussfaktoren: Feld der IT im Unternehmen

Unter „generellen Vorgaben“ sind interne Vorgaben zu sehen, die das Unternehmen sich selbst gibt, um seine Geschäftsziele optimiert verfolgen zu können. Hierzu zählen naturgemäß Vorgaben der Unternehmensstrategie, aus denen sich dann wiederum strategische Vorgaben für die IT und die Kommunikation ableiten. Auch weitere strategische Vorgaben wie z.B. die Sourcingstrategie bestimmen sich hieraus. Ein wesentlicher Faktor sind zur Verfügung stehende Ressourcen, insbesondere Budget und Personalressourcen. Weiterhin ist als Umsetzungsvorgabe der Unternehmensziele die Unternehmens-Governance zu beachten.

Eine große Rolle spielen die „Beteiligten“, also die im Umfeld der IT-Lösungen agierenden Menschen. Zunächst sind hier natürlich die IT-Anwender zu nennen. Auf die Ausprägung einer IT-Unterstützung nehmen jedoch auch Einfluss – unmittelbar oder mittelbar – Unternehmensleitung, Aktionäre und Mitbestimmung. Es gibt Einflüsse aus der Gesellschaft im Umfeld des Unternehmens wie z.B.: Bevölkerung, Kommunen, Anwohner und Kunden, deren Akzeptanz von großer Bedeutung ist. Faktisch wird die Ausprägung einer IT-Lösung immer auch von den (verfügbaren) Know-How-Trägern in der IT bestimmt.

Die „Rahmenbedingungen“, die das Handeln des Unternehmens bestimmen, nehmen immer auch Einfluss auf die IT-Unterstützung der Prozesse. Hier sind vor allem Vorgaben des Gesetzgebers zu nennen, aber auch Erfordernisse des Risikomanagements oder Anforderungen des gesellschaftlichen Umfeldes, z.B. hinsichtlich Umweltschutz.

Nicht zuletzt muss die IT den an sie gestellten „Leistungszielen“ entsprechen, offen erkennbar in der geforderten IT-Funktionalität und –Verfügbarkeit (z.B. definiert in entsprechenden Service Level Agreements). Kosten- und Budgetziele sind einzuhalten. Qualitative Merkmale einer IT-Unterstützung werden gefasst in den Begriffen Business/ IT Alignment, IT Capabilities oder Integration.

Für die IT ergibt sich somit ein mehrdimensionales Spannungsfeld. Es wird deutlich, dass eine IT-Lösung nicht allein die aus der unmittelbaren fachlichen Aufgabenstellung herrührenden Anforderungen zu bedienen hat, sondern dass zugleich eine Reihe andere Einflussfaktoren zu berücksichtigen sind.

Die im Kontext dieses Vortrages zu stellende Frage ist, ob der Ansatz des Cloud-Computing hier Perspektiven für Verbesserungen eröffnet. Anders ausgedrückt, eröffnen sich durch dieses Konzept neue Chancen, und können die ebenfalls damit verbundenen Risiken beherrscht werden? Im Folgenden (Bild 11) sollen zunächst exemplarisch wichtige mit Cloud-Computing verbundene Risiken diskutiert werden, um danach die sich bietenden Chancen näher zu betrachten.

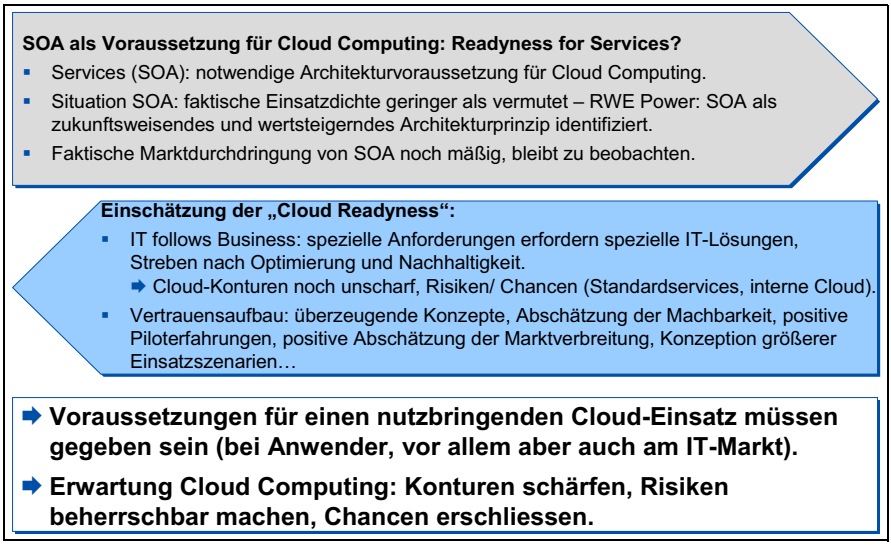


Bild 11: Bewertung aus Sicht RWE Power

Mit der Haltung von Daten in einer public-Cloud stellen sich zunächst Sicherheitsfragen. Sie zielen u.a. ab auf den Schutz der Daten vor Verlust, die Sicherung der Zugriffsmöglichkeit und auf die Verfügbarkeit. Der Schutz vor unbefugtem Zugriff (Datendiebstahl, unbefugtes Kopieren, Integrität, Vertraulichkeit) ist zu betrachten. Je wichtiger die Daten für die Kernprozesse eines Unternehmens sind, umso höher ist dieses Risiko naturgemäß zu bewerten. Wie bereits ausgeführt, sind hierbei auch gesetzliche Vorgaben zu beachten wie z.B. das Bundes-Daten-Schutz-Gesetz (BDSG).

Bei der Bewertung dieser Risiken hilft die Klarwerdung, dass der Daten- und Prozesseigentümer hier in jedem Fall die Verantwortung trägt – sowohl sich selbst gegenüber als auch anderen und insbesondere dem Gesetzgeber gegenüber.

Verfügbarkeit setzt IT-Connectivity voraus. Sie muss in jedem Fall den Anforderungen des Geschäftsprozesses genügen, denn eine Nichtverfügbarkeit der IT kann eine Nichtdurchführbarkeit des Geschäftsprozesses bedeuten. In eine entsprechende Risikoanalyse ist nicht nur der Cloud-Dienstleister einzubeziehen, sondern z.B. auch die Verbindung zwischen den Cloud-Rechenzentren und dem IT-Arbeitsplatz des Nutzers.

Ein weiteres, mögliches Risiko besteht in der Abhängigkeit vom Cloud-Dienstleister. Welche Möglichkeiten zum Dienstleisterwechsel bestehen? Wie einfach ist es, einen Applikations- und Datentransfer zu einem anderen Dienstleister zu erreichen? Von Interesse werden hier nicht allein die vertraglichen Gestaltungsmöglich-

keiten, sondern naturgemäß auch Erfahrungen zur praktischen Durchführbarkeit sein. Kritisch sind hierbei auch die Know- How-Träger, denn viele Prozesse und deren IT-Unterstützung bedingen spezielles Know How.

Ein weiteres Merkmal mit hohem Stellenwert für RWE Power ist – wie beschrieben – die Nachhaltigkeit eines Verfahrens zur Prozessunterstützung. Die Natur der langfristigen ausgerichteten Prozesse bei RWE Power stellt entsprechende Anforderungen auch an deren IT-Unterstützung. Beispielweise haben Datenbestände Relevanz über sehr lange Zeiträume und müssen entsprechend nachhaltig verfügbar sein.

Den aufgezeigten Risiken eines Einsatzes von Cloud-Computing stehen neue Chancen gegenüber. Ein Leistungsbezug aus der Cloud erscheint insbesondere im Bereich kostengünstiger IT-Commodity für klar definierte, standardisierte und kompakte Services, die über definierte Schnittstellen adressiert werden können, als interessantes Konzept – Erfüllung der Anforderungen hinsichtlich Interoperabilität und Sicherheitsanforderungen (siehe oben) vorausgesetzt.

Betrachtet man eine unternehmens- oder konzerninterne Cloud (private-Cloud), so sind die Sicherheitsfragen einfacher zu beantworten als bei einer externen (public-) Cloud. Mit ersten Erfahrungen einer sicheren private-Cloud werden sich Vorteile der Cloud-Architektur für große Unternehmen besser bewerten lassen und bei Erfolg, den Übergang zur Nutzung von Services aus der public-Cloud erleichtern.

Offenkundige Vorteile kann ein Service-Bezug aus der Cloud dann bieten, wenn es sich um nur von Zeit zu Zeit benötigte Funktionen handelt, die nach effektiver Nutzung abgerechnet werden – dies erspart eine aufwendigere, eigene Vorhaltung solcher IT-Funktionalitäten. Dieser Aspekt wird vor allem kleineren und mittleren Unternehmen große Vorteile eröffnen, die keine eigenen Skaleneffekte generieren können.

Zusammenfassend bleibt als Chance des Cloud-Computing festzuhalten, dass das Konzept Kosteneinsparungspotentiale eröffnen kann, im Gegenzug aber die möglichen Risiken beherrscht werden müssen. Die hier als Voraussetzung dargestellte SOA ist derzeit weder bei IT-Anbietern noch bei IT-Anwendern weit verbreitet sondern eher noch im Aufbau. Auch gibt es zurzeit noch unterschiedliche Einschätzungen zur Entwicklung der Marktverbreitung von Cloud-Computing, die für die genannten, positiven Effekte zwingende Voraussetzung ist.

Mit dieser Neuerung Cloud-Computing sind wieder Chancen und Risiken verbunden, die zu betrachten und abzuwägen sind. Auch hier kann sich das Neue bei am Markt agierenden Unternehmen dann gut verbreiten, wenn unter Abwägung aller für das Geschäft relevanten Aspekte eine Vorteilhaftigkeit leicht nachweisbar und natürlich eine Vertrauensbasis gegeben sind. Vertrauen in Neues wie hier

Cloud-Computing muss wachsen und erfordert Transparenz. In einem evolutionären Vorgehen muss sich Schritt für Schritt die Vorteilhaftigkeit des Neuen erweisen und so das Vertrauen für weitere Schritte aufbauen. Schlüsselfaktor wird dabei Transparenz sein, die primär seitens der Cloud-Serviceanbieter geschaffen werden muss.

4 Vernebeltes Vertrauen? Cloud Computing aus Sicht der Vertrauensforschung

Dr. Guido Möllering
Max-Planck-Institut für Gesellschaftsforschung, Köln

Es ist eine Ehre und auch eine Herausforderung, bei dieser Fachkonferenz, in deren Zentrum vor allem technische und technologische Fragen stehen, die Sichtweise der sozialwissenschaftlichen Vertrauensforschung zu vertreten und Ihnen näher zu bringen. Es spricht für sich – oder besser gesagt: es spricht für Sie, dass Sie das innovative Thema Cloud Computing mit einem Klassiker des menschlichen Zusammenlebens und Zusammenarbeitens verknüpfen, nämlich mit Vertrauen. Klingt dieser Begriff – Vertrauen – in Ihren Ohren nicht ein wenig verstaubt, altmodisch oder gar weltfremd? Brauchen wir ihn wirklich, wenn wir über die neuesten und fortschrittlichsten Informationstechnologien sprechen? Uns allen hier im Saal sollte klar sein, dass Cloud Computing nicht losgelöst von sozialen Kontexten und Beziehungen stattfindet und dass eben gerade auch im Internet die Bedingungen der Ungewissheit und Verwundbarkeit gegeben sind, die Vertrauen als Problem und zugleich als dessen Lösung ins Spiel bringen.

Das Bild der Wolke

„Cloud" Computing, Informationsverarbeitung in der Internet „Wolke". Inzwischen nimmt man vom Bild der Wolke vielleicht kaum noch Notiz. Man verwendet in Diagrammen ohne weiteres das Wolkensymbol für das Internet. Ich lade Sie ein, dieses Bild der Wolke einmal wieder ernst zu nehmen. Die Problematik des Vertrauens im Cloud Computing lässt sich nämlich damit schon sehr schön in einem ersten Zugang erschließen. Stellen Sie sich bitte vor, wie es ist, wenn man mit dem Flugzeug in eine Wolke fliegt, als Wanderer oder vielleicht auch als Skifahrer im Gebirge von einer Wolke eingeschlossen wird, oder wenn man mit dem Auto in den Nebel fährt. Man sieht dann kaum noch die anderen Akteure – also die anderen Flugzeuge, Wanderer, Skifahrer, Autos – und was sie tun. Man verliert gar die Orientierung und kann sich nur mit großer Vorsicht fortbewegen. Man sucht vor allem auch nach Orientierungspunkten. Mit Radar, GPS und Nebelscheinwerfern wird die Situation dank technischer Hilfsmittel um einiges ungefährlicher. Jedoch bleibt die Sorge, dass andere Akteure fahrlässig oder gar böswillig im Nebel unterwegs sein könnten. Ohne Vertrauen, müsste man wohl auf der Stelle stehen bleiben und wäre selbst dann nicht in Sicherheit. Oder man müsste jede Wolke und jede

A. Picot et al. (eds.), *Trust in IT*, DOI 10.1007/978-3-642-18110-8_4,

Nebelbank meiden – und alle Chancen, die darin liegen, verpassen. Auch in der Internet Wolke haben wir vergleichsweise „schlechte Sicht“, können die anderen Akteure nur zum Teil kennen und kontrollieren und stoßen mit unseren technischen Hilfsmitteln immer wieder an Grenzen. Vertrauen macht Kooperation unter diesen Umständen möglich, ist selbst jedoch unter solchen Umständen schwerer aufzubauen und zu erhalten. Der Nebel kann nicht beseitigt werden und die Technologien sind nicht perfekt, aber wir können Orientierungspunkte für Vertrauen schaffen.

Vertrauensforschung

Bevor ich auf die Besonderheiten des Vertrauens im Cloud Computing eingehe, gestatten Sie mir noch einige Anmerkungen zur Vertrauensforschung im Allgemeinen. Die (eine) Vertrauensforschung als ein klar abgegrenztes, homogenes Feld gibt es gar nicht. Es handelt sich vielmehr um ein ausgesprochen heterogenes Feld, auf dem sich Wissenschaftler aus den verschiedensten Disziplinen tummeln und alle möglichen Forschungsfragen bearbeiten, die mit Vertrauen zu tun haben. Zwar gibt es auch gemeinsame Bezugspunkte – in Deutschland kommt man zum Beispiel kaum an dem kleinen, sehr scharfsinnigen Buch zu Vertrauen von Niklas Luhmann vorbei – doch oft widmen sich Forscher dem Thema eher ad hoc und improvisieren bei den theoretischen und methodischen Grundlagen, statt auf eine Art Kanon zurückzugreifen. Den gibt es schlichtweg noch nicht, auch wenn hier und da schon Handbücher zu Vertrauen herausgegeben wurden (vgl. Literaturhinweise hinten).

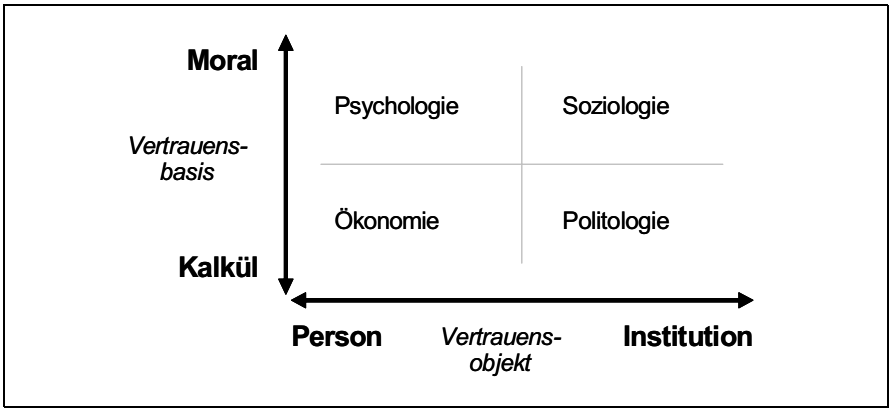


Bild 1: Sozialwissenschaftliche Vertrauensforschung

Vertrauen ist vor allem eine soziale Kategorie – zumindest auch, wenn man vom Alltagsverständnis des Begriffes ausgeht. Es geht um Beziehungen zwischen Akteuren, die sich gegenseitig wahrnehmen und dies in ihrem Handeln berücksichtigen. Und so ist es kaum verwunderlich, dass sich vor allem die Sozialwissenschaften mit

diesem Thema befassen. Hier wiederum kann man stark vereinfachend die in Bild 1 dargestellte Systematik beobachten. Ein Teil der Forscher – insbesondere in der Ökonomie und der Politikwissenschaft – sieht als Basis des Vertrauens vor allem ein Kalkül, während andere Wissenschaftler – vor allem Psychologen und Soziologen – moralische und emotionale Grundlagen von Vertrauen betonen. In einer zweiten Dimension kann man unterscheiden, ob es um Vertrauen in Personen oder Vertrauen in Institutionen geht. Hier stehen sich die Ökonomie und die Psychologie nahe, weil sie meist Interaktionen zwischen konkreten Akteuren vor Augen haben, während die Politologen und Soziologen eher abstrakte Vertrauensobjekte betrachten.

Man muss natürlich hinzufügen, dass die Grenzen zwischen den Disziplinen hier auch fließend sind. Ich selbst habe mich von Anfang an einem interdisziplinären Ansatz verschieben. Es bringt wenig, sich darüber zu streiten, in welcher der vier Ecken das „echte“ Vertrauen steckt. Vielmehr geht es in dem ganzen Feld darum, positive Erwartungen trotz Ungewissheit und Verwundbarkeit zu erklären. Also sollte man auch Erkenntnisse aus allen Disziplinen nutzen. Vielleicht kommt hier zum Ausdruck, dass ich ein Organisationsforscher aus der BWL bin. Leute wie ich beschäftigen sich eben meist mit Organisationen auf einer mittleren Ebene zwischen Mikro- und Makroebene und analysieren vor allem auch das Zusammenspiel von Mikro und Makro. Und die BWL als anwendungsorientierte Wissenschaft kann es sich gar nicht leisten, die reine Theorie zu pflegen, sondern muss realitätsnah für alle Einflussfaktoren offen sein, auch wenn sie in einer ungewohnten Disziplin entdeckt wurden.

Diese Offenheit gilt grundsätzlich auch gegenüber den Natur- und Ingenieurwissenschaften, die ebenfalls etwas zu Vertrauen zu sagen haben. In den Naturwissenschaften ist dies vor allem die neurowissenschaftliche Forschung, die viel Aufmerksamkeit erhält und durchaus interessant ist. Allerdings muss ich gestehen, dass mir zum Beispiel Studien darüber, welche Hirnareale in simulierten Vertrauenssituationen besonders aktiv sind, noch keine Erklärungen für Vertrauen geliefert haben, auf die man nicht auch schon mit anderen Methoden gekommen wäre. Das gilt auch für die Studien über sogenannte Vertrauenshormone. Hier sehe ich es sogar mit Sorge, dass man einmal auf die Idee kommen könnte, Oxytocin-Sprays zu verteilen. Momentan ist es noch schwer, den Oxytocin-Spiegel bei Menschen künstlich zu erhöhen, doch die Pharmaforschung kann da bestimmt helfen. Aber wollen wir das Vertrauen im Internet mit Drogen steigern? Oder durch Aufrufe, wie sie zumindest halbernst aus den USA kommen, die Leute müssten einfach mehr kuscheln, weil sie dann mehr Hormone im Blut haben, die Vertrauen bewirken?

In den Ingenieurwissenschaften gibt es Beiträge zur Vertrauensforschung gerade auch im Bereich der neuen Informationstechnologien. Man beschäftigt sich hier – nah an der Ökonomie – zum Beispiel mit Zertifizierungssystemen und Reputationsmechanismen. Außerdem gibt es Studien – näher an der Psychologie – die vereinfacht gesagt analysieren, wie Vertrauensbereitschaft mit Webdesign zusammen-

hängt. Zuletzt erwähnt seien hier noch die vielfältigen Forschungen darüber, wie man gefälschte Daten automatisch erkennen kann, was sicherlich auch für das Thema Cloud Computing relevant ist. Diese Art der Forschung macht sehr viel Sinn, jedoch muss ich aus einer allgemeinen Perspektive der Vertrauensforschung kritisieren, dass hier häufig nicht zum Kern der Vertrauensproblematik vorgedrungen wird, sondern man an der technischen Oberfläche bleibt. Was aber ist der Kern der Vertrauensproblematik? Was macht Vertrauen aus? Vor allem: Wie kann man es definieren?

Definition von Vertrauen

Ich beanspruche selbstverständlich keine Allgemeingültigkeit, jedoch schlage ich vor, von folgender allgemeinen Definition auszugehen: Vertrauen bedeutet, trotz Ungewissheit und Verwundbarkeit zu erwarten, dass andere ihre Freiräume kompetent und verantwortungsvoll nutzen. Diese kurze Definition hat es in sich. Schauen wir uns das einmal genauer an. Beim Vertrauen geht es also um positive Erwartungen. Die anderen, in die die Erwartungen gesetzt werden, können sehr spezifische Personen oder aber eher abstrakte Akteure sein. Das spielt hier zunächst noch keine große Rolle, darauf komme ich aber noch zurück.

Wichtiger ist mir hier zunächst, erstens, dass Vertrauen sich auf die Freiräume der anderen bezieht. Diese Freiräume werden also vorausgesetzt oder, anders ausgedrückt: Wenn andere keine Freiräume haben, dann braucht man ihnen auch nicht zu vertrauen. Dann hat man ja vollkommene Sicherheit. Wenn Sie meinen, dass Cloud Computing nur dann funktioniert, wenn die Beteiligten gar keine Freiräume haben, um eventuell in irgendeiner Weise unkooperativ zu handeln, dann reden wir einseitig von Kontrolle und haben es eigentlich gar nicht mehr mit Vertrauen zu tun. Wenn wir allerdings davon ausgehen, dass immer Freiräume bleiben werden und dass dies sogar sehr wünschenswert ist, denn wir schätzen am Internet ja gerade auch seine Offenheit und Flexibilität, dann sehen wir unmittelbar wieder die Notwendigkeit des Vertrauens.

Zweiten ist Vertrauen als positive Erwartungshaltung nicht naiv oder bedingungslos. Die Definition verweist auf Kompetenz und Verantwortungsbereitschaft. Diese will der Vertrauensgeber beim Vertrauensnehmer sehen. Erweist sich der Vertrauensnehmer als inkompetent oder übernimmt er beim Auftreten von Problemen und Fehlern keine Verantwortung oder erfüllt er ganz allgemein die positiven Erwartungen nicht, dann kann Vertrauen natürlich auch wieder entzogen werden. Doch zunächst gibt Vertrauen dem anderen die Chance, sich freiwillig als vertrauenswürdig zu erweisen, indem er seine Freiräume nicht missbraucht.

Drittens steckt im Phänomen des Vertrauens noch eine ganz spezielle Eigenheit, geradezu eine Zumutung: Vertrauen ist eine positive Erwartung trotz Ungewissheit und Verwundbarkeit. Vertrauen wird erst unter den Bedingungen der Ungewissheit

und Verwundbarkeit relevant und setzt sich dann quasi über diese hinweg. Der Vertrauende weiß also nicht mit Sicherheit, wie der andere seine Freiräume nutzen wird, und ein Missbrauch würde dem Vertrauenden auch schaden. Aber er nimmt dennoch das Beste an und gibt der Kooperation eine Chance. Er tut dies nicht blind, hat dafür gute Gründe, aber eben keine perfekten Gründe. Es bleibt eine Lücke, die mit Vertrauen überbrückt wird. Es bleibt der Nebel, man bleibt vorsichtig, aber man bewegt sich trotzdem. Man handelt, als ob man wüsste, dass alles gut gehen wird. Und schon wieder wirkt Vertrauen naiv und weltfremd, doch ich sage Ihnen: Nein, Vertrauen dieser Art macht handlungsfähig und ist außerdem ganz alltäglich.

Ich bin gerne bereit, dieses Vertrauensverständnis mit Ihnen weiter zu diskutieren. Für die heutige Fachkonferenz möchte ich an dieser Stelle folgende Anregung festhalten: Denken Sie darüber nach, welchen Status die Freiräume der Akteure im Cloud Computing haben. Und machen Sie sich stets bewusst, ob es in Ihren Diskussionen um die Begrenzung oder Ausweitung dieser Freiräume geht. Oder ob es um die Akzeptanz der Freiräume und um deren kompetente und verantwortungsvolle Nutzung geht. Verwechseln Sie also nicht Kontrolle mit Vertrauen und vergessen Sie nicht, dass Kontrolle und Vertrauen beide nötig sind.

Generalisiertes Vertrauen

Ich komme nun zu einigen Besonderheiten des Vertrauens im Cloud Computing und werde mich dabei im Wesentlichen auf zwei Hauptpunkte beschränken: Zum einen ist im Cloud Computing das generalisierte Vertrauen besonders wichtig, da spezifisches Vertrauen schwer aufzubauen ist. Zum anderen geht es vor allem um Vertrauen in ein abstraktes System und weit weniger um Vertrauen in individuelle Akteure. Gerade dieses diffuse Vertrauen im Cloud Computing ist eine Art Kollektivgut, zu dem die Einzelnen beitragen müssen. Dabei geht es nicht so sehr um „Anbieter gegen Nachfrager“ als um eine Koalition der Verantwortungsvollen gegen Betrüger und Trittbrettfahrer.

Beim Cloud Computing sind natürlich viele Varianten vorstellbar, aber lassen Sie uns internettypisch von einem relativ offenen System ausgehen. Die Teilnehmer begeben sich also in die besagte Wolke mit vielen anderen Teilnehmern. Soweit man im Cloud Computing nicht genau wissen kann, welche Akteure an dem System beteiligt sind und welche individuellen Anreize ihr Handeln bestimmen, so kann man Vertrauen nicht kalkulierend und fallweise produzieren, sondern braucht eine vertrauensvolle Grundeinstellung, die auch als generalisiertes Vertrauen bezeichnet wird. Damit ist die Annahme gemeint, dass andere Akteure im Allgemeinen vertrauenswürdig sind und man sich im Zweifel eher für als gegen Kooperation entscheidet.

Das Konzept des generalisierten Vertrauens wird bereits seit den späten 1940er Jahren in der empirischen Forschung eingesetzt und zwar inzwischen weltweit. Man stellt in den entsprechenden Erhebungen zumeist folgende Frage: „Manche

Menschen sagen, dass man den meisten Menschen trauen kann. Andere meinen, dass man nicht vorsichtig genug sein kann im Umgang mit anderen Menschen. Was ist Ihre Meinung dazu?“ Fragen Sie sich bitte einmal, welche Antwort Sie geben würden: Man kann den meisten Menschen vertrauen? Oder: Man kann nicht vorsichtig genug sein? – In Deutschland antworten übrigens gut 30%, dass man vertrauen kann, und etwa 60% sind lieber vorsichtig. Damit liegt Deutschland im Mittelfeld, gehört aber schon zu den Ländern mit eher hohem generalisiertem Vertrauen.

Im Cloud Computing würde generalisiertes Vertrauen also bedeuten, dass die Teilnehmer meinen, dass man den meisten anderen Teilnehmern in diesem System vertrauen kann. Ein solches generalisiertes Vertrauen ist vor allem moralisch fundiert und wird durch gute Erfahrungen bestätigt. Diese Art des Vertrauens gründet sich wohlgemerkt nicht darin, dass man die anderen Teilnehmer durchschauen und kontrollieren kann. Natürlich ist es auch nicht schädlich, wenn man zu einigen Teilnehmern bereits eine engere Beziehung hat, die gut funktioniert. Dies darf jedoch nicht verhindern, dass man auch eher unbekannte Teilnehmer in das System hineinlässt, die sich dann natürlich als vertrauenswürdig erweisen müssen, denen man jedoch einen Vertrauensvorschuss gewährt.

Jeder Teilnehmer sichert durch sein vertrauenswürdiges Verhalten nicht nur seinen eigenen Zugang zu dem System, sondern reproduziert und stärkt auch das generalisierte Vertrauen der anderen. Und damit der Vertrauensmissbrauch einzelner Teilnehmer nicht das generalisierte Vertrauen zerstört, müssen Vertrauensbrecher auch konsequent aus dem System wieder ausgeschlossen werden oder – falls das nicht so ohne weiteres möglich ist – unter besondere Beobachtung gestellt werden, bis sie die Erwartungen wieder erfüllen. Generalisiertes Vertrauen fällt also nicht vom Himmel, sondern muss gepflegt werden.

Entwicklungspsychologisch gesprochen steht das generalisierte Vertrauen dem sogenannten Urvertrauen nahe, das sich im Kleinkindalter entwickelt. Diese „Früherziehung zum Vertrauen“ ist aus der Sicht des Cloud Computing recht weit weg. Aber sie ist doch in sofern noch übertragbar, dass gerade in der frühen Phase in der Etablierung eines System – und gerade in Bezug auf Neueinsteiger in das System – besonders in Vertrauen investiert werden muss. Das bedeutet: in die Etablierung eines Musters, wonach Freiräume selbstverständlich gewährt, aber ebenso selbstverständlich auch nicht missbraucht werden. Verstöße müssen in dieser Phase unbedingt geahndet werden, aber nicht direkt zum Ausschluss führen. Gerade das Zugestehen einer zweiten Chance kann nämlich Vertrauen fördern.

Ich frage mich – und ich frage Sie, ob es vorstellbar ist, die Cloud Computing Systeme grundsätzlich „kooperationsfreundlich“ zu programmierten. Dazu würde dann eben auch eine gewisse Fehlertoleranz gehören sowie eine Kultur des konstruktiven Problemlösens. In der Vertrauensforschung hat sich immer wieder gezeigt, dass

Vertrauen durch gemeinsames Problemlösen gestärkt wird. Und es wird mithin nicht schon dadurch zerstört, dass ein Problem auftritt, sondern erst dadurch, dass die betreffenden Akteure das Problem nicht lösen, sondern sich als inkompetent erweisen oder sich gar ihrer Verantwortung entziehen. Anbieter von Cloud Computing Diensten sollten also besonderen Wert auf ihren User Support und Kundenservice legen. Und die Kunden sollten nicht gleich beim ersten Problem den Anbieter wechseln, sondern ihrerseits konstruktiv zur Problemlösung beitragen. Wenn diese Grundeinstellung weit verbreitet ist, dann steht es um das generalisierte Vertrauen bereits gar nicht schlecht. Wohlgemerkt geht es ja nicht nur darum, dass man selbst Wechsel- oder Neuanwerbungskosten sparen kann, sondern dass man mit seinem kooperativen Verhalten auch die Vertrauenskultur in dem System pflegt.

Vertrauen in abstrakte Systeme

Das System der Internet Cloud ist zudem ein abstraktes System, in dem einzelne Akteure zumeist nur einen kleinen Teil der Leistung beitragen und verantworten können. Das System als Ganzes darf man sich wiederum nicht als einen Akteur vorstellen, der sich schlüssig und konsistent entscheidet, das in ihn gesetzte Vertrauen zu honorieren oder zu brechen. Die Vertrauensforschung weist vielmehr darauf hin, dass Vertrauen in ein abstraktes System dadurch aufgebaut und gepflegt wird, dass die Repräsentanten an den Zugangspunkten und die das System kontrollierenden Experten vertrauenswürdig sind. Das Vertrauensobjekt bleibt nach wie vor das System, doch die Vertrauenswürdigkeit des Systems macht der Vertrauensgeber am Verhalten bestimmter Akteure fest.

Ich beziehe mich hierbei insbesondere auf Überlegungen von Anthony Giddens und Niklas Luhmann. Giddens betont die Bedeutung von sogenannten Zugangspunkten zu abstrakten Systemen. Und diese Zugangspunkte sind eben oft Personen. Beim Gesundheitssystem ist es etwa das medizinische Personal, beim Luftverkehrssystem sind es unter anderem die Flugbegleiter und bei unserem Regierungssystem sind es die Bundeskanzlerin und die Minister. In allen Fällen beobachtet der Vertrauensgeber diese Repräsentanten, um zu sehen, ob das abstrakte System noch vertrauenswürdig ist. Entsprechend legen diese Repräsentanten besonderen Wert auf ihr Auftreten. Bleiben wir bei Giddens, der das Beispiel der Stewardessen anführt: Durch ihr freundliches Lächeln, ihre Kleidung, die Selbstverständlichkeit, mit der sie den Flug vorbereiten, signalisieren sie uns – ganz bewusst – dass alles in Ordnung ist mit dem Flugzeug und dem ganzen Drumherum. Stellen sie sich einmal vor, dass Sie eine schlecht gekleidete, unfreundliche und unsichere Person im Flugzeug begrüßt und etwas über die widrige Witterung und die komischen Geräusche am Fahrwerk murmelt. Wir durchschauen das System nicht, aber an diesem Zugangspunkt wollen wir die Bestätigung, dass alles gut geht, und keine Erinnerung an die verbleibende Ungewissheit und Verwundbarkeit.

Bei Luhmann, der ansonsten in vielen Punkten Vertrauen anders versteht als Giddens, finden sich einige Überlegungen zum Systemvertrauen, die den vorigen Gedanken unterstützen und erweitern. Luhmann verweist darauf, dass Vertrauen in ein System vor allem durch Vertrauen in die in das System eingebauten Kontrollen gestützt wird. Das ist interessant, weil hier Vertrauen durch Kontrolle produziert wird, aber man achte auf die Feinheiten. Der Vertrauende ist keineswegs in der Lage, dass System selbst zu kontrollieren. Er muss ihm nach wie vor vertrauen. Er weiß jedoch, dass in das System Kontrollen eingebaut wurden. Nun kann sich sein Vertrauen darauf konzentrieren, dass diese Kontrollen funktionieren. Ich würde sagen, dass dies auf einen besonderen Typus eines Zugangspunktes zum System verweist, nämlich auf die Kontrolleure. Man vertraut dem System, weil man den Kontrolleuren des Systems vertraut, die aber doch selbst Teil des Systems sind.

Zusammenfassend finde ich hier zwei Aspekte für die weiteren Diskussionen besonders wichtig. Erstens: Beim Vertrauen in abstrakte Systeme handelt es sich nicht um ein indirektes Vertrauen vermittelt durch spezifische Personen. Ich muss die Ärztin, die Stewardess oder die Lebensmittelkontrolleurin nicht persönlich kennen, aber ihr persönliches Verhalten gibt mir wichtige Signale über das System. Es geht also, wie auch beim generalisierten Vertrauen, nicht nur um konkrete Beziehungen, sondern um das Vertrauen darüber hinaus.

Zweitens: Eingebaute Kontrollen können vertrauensförderlich sein und sie sind zweifelsohne auch im Cloud Computing nötig. Jedoch wird man Opportunismus und Fehler wohl niemals völlig ausschließen können. Und die Betonung der Vertrauenswürdigkeit der Kontrolleure bedeutet ja vor allem eine teilweise Verschiebung der Vertrauensproblematik vom System zu den Kontrolleuren. Und wer kontrolliert bitte die Kontrolleure?

Fazit: Verantwortung zeigen

So wird es auch im Cloud Computing über alle Bemühungen um fehlerfreie Technologien, lückenlose Rechtsapparate, konsequente Aufsichtsinstanzen und vorsorgliche Versicherungen hinaus immer nötig sein, dass die Beteiligten signalisieren, dass sie Verantwortung für das System tragen wollen – auch über ihre individuellen Verpflichtungen hinaus. Geschieht dies, werden sich viele weitere Akteure in die Wolke hineinwagen. Ich habe in meinem Vortrag herausgestellt, dass es in der Internet Cloud vor allem auf generalisiertes Vertrauen und Vertrauen in abstrakte Systeme ankommt. Wo technische Sicherungsmechanismen an Grenzen stoßen, müssen die verbleibenden Lücken durch soziale Mechanismen geschlossen werden. Daher gilt es, Gelegenheiten zu schaffen und zu nutzen, bei denen die das System tragenden Akteure in Erscheinung treten, ihre Verantwortungsbereitschaft beweisen und auch gegen die vorgehen, die verantwortungslos handeln – egal, ob diese auf der Seite der Anbieter, der Nachfrager oder der Behörden stehen. Es geht

nicht um absolute Sicherheit, sondern um den guten Willen. Der allein reicht wiederum auch nicht aus – das wäre ja weltfremd – aber er muss stets erkennbar sein, wenn Cloud Computing mit Vertrauen effizienter oder überhaupt erst in der Breite möglich werden soll.

Der Autor

Dr. Guido Möllering ist Wissenschaftlicher Mitarbeiter am Max-Planck-Institut für Gesellschaftsforschung in Köln. Er wurde 2003 an der Universität Cambridge promoviert und forscht über Vertrauen, Unternehmenskooperation und Marktkonstitution. Weitere Informationen: www.mpifg.de/people/gm.

Literaturhinweise

Bachmann, Reinhard / Zaheer, Akbar (Hrsg.), 2006: Handbook of Trust Research. Cheltenham: Edward Elgar.

Giddens, Anthony, 1999. Konsequenzen der Moderne. 3. Aufl., Frankfurt/M.: Suhrkamp.

Latusek, Dominika / Gerbasi, Alexandra, 2010: Trust and Technology in a Ubiquitous Modern Environment. Hershey, PA: Information Science Publishers.

Luhmann, Niklas, 2000: Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität. 4. Aufl., Stuttgart: UTB.

Möllering, Guido, 2006: Trust: Reason, Routine, Reflexivity. Oxford: Elsevier.

Zak, Paul, 2009. Die Neurobiologie des Vertrauens. In: Spektrum der Wissenschaft, Heft 04/09 (April), S. 40-46.

5 Gelöste und ungelöste Rechtsfragen im IT-Outsourcing und Cloud Computing

Dr. Alexander Duisberg
Bird & Bird LLP, München

1. Einleitung

Mit dem Phänomen des Cloud Computing setzt sich die Diskussion um Rechtsfragen der Auslagerung und Virtualisierung von IT-Dienstleistungen fort und erreicht in einigen Aspekten eine neue Dimension. Die universelle Verknüpfung von Rechenzentren und Rechenleistungen aufgrund entsprechender Breitbandverbindungen verleiht dem Schlagwort des Cloud Computing – und den damit bezeichneten Dienstleistungen von Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS) – eine Faszination, die auch die Fantasie der Juristen im nationalen und internationalen Kontext beflügelt. Auf der Grundlage der für das „klassische" IT-Outsourcing gefundenen Ansätze lässt sich Neues – oder scheinbar Neues – im Bereich des Cloud Computing vielfach auf bekannte Prinzipien zurückführen. Die bei rasanter Technologieentwicklung oftmals kaum nachvollziehbare, grenzüberschreitende Kopplung von Rechenleistungen und Software-Bereitstellung auf der Basis On-demand-basierter Geschäftsmodelle stellt aber auch neue Anforderungen an die Vertragsgestaltung, regulatorische „Compliance" und die Absicherung der damit verbundenen Risiken.

Im Folgenden sollen einige der Kernfragen angesprochen werden, die derzeit die Anbieter ebenso wie die gewerblichen und privaten Nutzer von Outsourcing und Cloud Computing beschäftigen. Gewerbliche Anbieter von Cloud Computing stehen dabei vor der Herausforderung, die praktisch globale Verfügbarkeit von IT-Leistungen – und die damit verbundenen Optimierungs- und Skaleneffekte – mit verschiedenen nationalen Rechtsordnungen innerhalb und außerhalb des EU-Rechtsrahmens in Einklang zu bringen. Dabei spielen über die vertragsrechtlichen und Compliance-Fragen hinaus zumindest auf der Kundenseite nicht zuletzt auch psychologische Aspekte eine kritische Rolle bei der Entscheidung für oder gegen ein Cloud Computing Angebot. In diesem Zusammenhang ist die Gewährleistung von Datenschutz und Datensicherheit fundamental, um die standortunabhängige Verknüpfung von Rechenleistungen mit legitimen Kundenanforderungen und -bedenken zu vereinbaren. Ein wichtiger vertrauensbildender Faktor liegt insbesondere in der vertraglichen Absicherung und Umsetzung der regulatorischen Anforderungen an den Umgang mit Sicherheitspannen.

A. Picot et al. (eds.), *Trust in IT*, DOI 10.1007/978-3-642-18110-8_5,

2. Public vs. Private Cloud

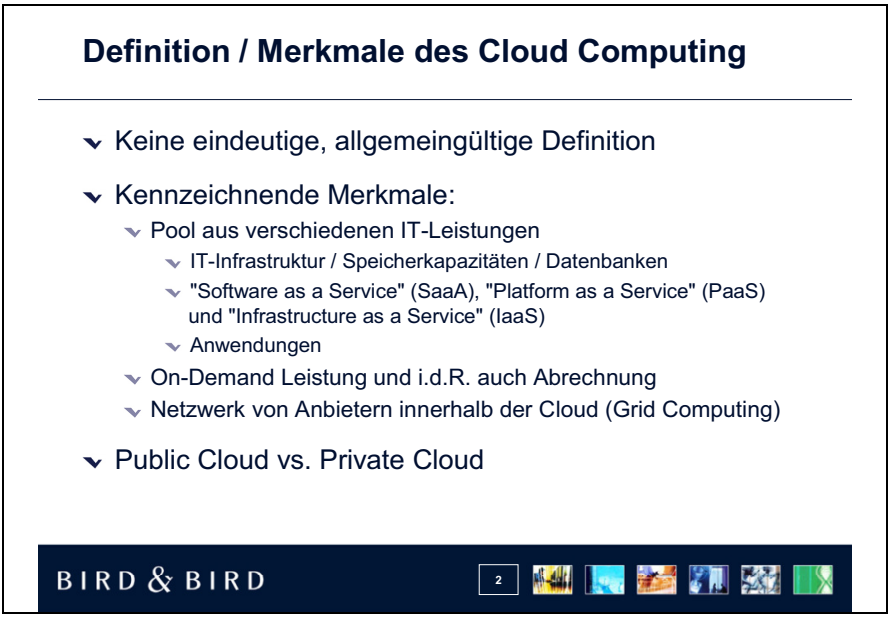


Bild 1

Auch in rechtlicher Hinsicht ist die Unterscheidung zwischen der „Public Cloud“ und der „Private Cloud“ von Bedeutung und führt zu unterschiedlichen Einordnungen und Folgen (Bild 1). Was zunächst als Vermarktungsstrategie der Anbieterseite erscheint, eröffnet unterschiedliche Gestaltungsmöglichkeiten und die Berücksichtigung von rechtlichen Anforderungen der Kundenseite. Während man unter der Public Cloud die jedermann zugängliche Abrufbarkeit von Rechenleistungen, IT-Infrastrukturdienstleistungen und Anwendungen für eine unbestimmte Vielzahl von Nutzern versteht, ermöglicht die Private Cloud eine spezifisch auf die Bedürfnisse eines einzelnen Kunden ausgerichtete virtualisierte Rechenumgebung. Dies gilt selbst dann, wenn „im Hintergrund der Private Cloud“ bestimmte Infrastrukturleistungen mehreren Kunden zur Verfügung gestellt werden und die Grundlage für dedizierte Private Clouds einzelner Kunden bilden (beispielsweise im Sinne eines Shared Service). Damit rückt die Private Cloud deutlich in die Nähe des herkömmlichen IT-Outsourcings.

Vertragsverhandlungen über Private Cloud-Angebote stehen typischerweise im Spannungsfeld zwischen den spezifischen Leistungsparametern und Compliance-Anforderungen des Kunden und einem hohen Standardisierungsgrad der angebotenen Leistung. In rechtlicher Hinsicht führt die Diskussion von der konkreten Beschreibung der Leistungen über Service-Levels und Pönalen, Haftungs- und

Gewährleistungsfragen, Sicherheitsstandards, Risikoabsicherungen im Bereich des Desaster-Recovery, der Verantwortung für integrierte Leistungen Dritter in der Regel zu einer differenzierten Vertragsgestaltung. Da Geschäftsmodelle im Bereich des Cloud Computing in hohem Maß auf Standardisierung und Skalierbarkeit fußen, liegt es auf der Hand, dass umfassende Abweichungen vom Standardangebot eine Kostenanalyse und Grenzwertbetrachtung des wirtschaftlichen Erfolgs des Private Cloud Computing auf Anbieterseite erfordern

3. Anwendbares Recht

Bild 2

Die Frage nach dem anwendbaren Recht lässt sich beim Cloud Computing – ebenso wie bei anderen web-basierten, grenzüberschreitenden Leistungsangeboten – in zwei Grundfragen gliedern (Bild 2): Es stellt sich zum einen die Frage des anwendbaren Vertragsrechts, das sich aus einer wirksamen Rechtswahl in den Vertragsbedingungen des Anbieters oder – in Ermangelung einer wirksamen Rechtswahl – aus dem jeweils anwendbaren internationalen Privatrecht[1] ergibt. Zum anderen geht es

[1] Als „internationales Privatrecht“ bezeichnet man diejenigen Regelungen einer nationalen Rechtsordnung, aus denen sich (unter anderem) ergibt, welches nationale Recht auf Verträge anzuwenden ist. Innerhalb der EU wurde das internationale Privatrecht mit Wirkung zum 17. Dezember 2009 vereinheitlicht (vgl. Fußnote 2).

um die Frage der Konformität der Leistungserbringung mit sämtlichen anwendbaren regulatorischen Anforderungen, die für ein einziges Cloud Angebot potenziell einer Vielzahl nationaler Rechtsordnungen entstammen können.

Für Rechtsbeziehungen zu Geschäftskunden gilt – auch im Rahmen von Standardverträgen bzw. Allgemeinen Geschäftsbedingungen – der Grundsatz der freien Rechtswahl, soweit das gewählte Recht in einer gewissen Beziehung entweder zum Leistungsort des Dienstleisters oder zum Sitz des Kunden steht. Stellt man auf den Leistungsort des Dienstleisters ab, liegt dieser allerdings bildlich gesprochen „in der Cloud". Rechtlich bleibt dies unproblematisch, soweit der Dienstleister einen eindeutigen Geschäftssitz hat und diesen kenntlich macht.

Schwieriger wird es, wenn Leistungen aus der Public Cloud nicht durch nationale, auf einzelne Länder oder Regionen ausgerichtete Internetseiten erfolgen, sondern als universelle Dienstleistung einheitlich angeboten werden. Aus der Sicht des deutschen (und europäischen) internationalen Privatrechts wird im Zweifel das Recht des Staates zur Anwendung kommen, in dem der Leistungserbringer „seinen gewöhnlichen Aufenthalt hat" (siehe Artikel 4 Abs. 1 b) Rom I)[2]. Sofern ein international auftretender Cloud-Dienstleister diese Angaben z.B. im Impressum seiner Internetseite macht (wie dies in Deutschland gemäß § 6 Telemediengesetz erforderlich ist), kommt man zu einer eindeutigen Anknüpfung. Das ist jedoch gerade bei ausländischen, nicht EU-basierten Anbietern – insbesondere Public Cloud basierter Leistungen – keineswegs immer der Fall, so dass eine eindeutige Rechtsanknüpfung scheitern kann.

Soweit sich Anbieter von Public Cloud- Leistungen an Verbraucher richten und in ihren Vertragsbedingungen atypische Rechtswahlklauseln vorsehen, dürften diese aus der Sicht des (gegenüber deutschen Verbrauchern weitgehend zwingenden) deutschen AGB-Rechts als überraschende Rechtswahlklauseln bereits an einer wirksamen Einbeziehung scheitern. Es gilt dann das Recht des Staates, in dem der Verbraucher ansässig ist[3]. Im Übrigen bleiben selbst im Falle einer wirksamen Rechtswahl zwingende nationale Verbraucherschutzregelungen stets zugunsten des Verbrauchers anwendbar (vgl. Art. 6 Abs. 2 Rom I).

In regulatorischer Hinsicht entfaltet eine zwischen den Parteien getroffene Rechtwahl keine Wirkung. Die Anwendbarkeit nationaler regulatorischer Vorgaben folgt vielmehr allein aus der Berührung von (Teil-)Leistungen mit dem Herrschaftsgebiet eines nationalen Staates. Die der Cloud wesenseigene Verknüpfung von Teilleis-

---

[2] Verordnung EG 593/2008 vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I), das seit dem 17. Dezember 2009 insoweit für den Bereich der EU die Bestimmungen des Art. 28 Abs. 2 Satz 1 EGBGB abgelöst hat.

[3] Für den EU Raum gilt dies gemäß Artikel 6 Abs. 1 b) Rom I jedenfalls dann, wenn das Cloud-Angebot zumindest auch auf die Jurisdiktion ausgerichtet ist, in der der Verbraucher seinen gewöhnlichen Aufenthalt hat (wie vormals durch Artikel 29 Abs. 2 EGBGB geregelt).

tungen unterschiedlicher geographischer Herkunft wirft daher die Frage auf, ob und wie sich der Zielkonflikt zwischen einer Vielzahl anwendbarer unterschiedlicher regulatorischer Anforderungen einerseits und der Standardisierung eines IT-Leistungsangebots „aus der Cloud" anderseits auflösen lässt. Für IT-Leistungen aus der Public Cloud muss man wohl davon ausgehen, dass die „Quadratur des Kreises" einer ubiquitären regulatorischen Compliance nicht gelingen wird. In der Private Cloud werden die Compliance-Anforderungen der einzelnen Kunden die Anbieterseite zwingen, ihre IaaS-, PaaS- und SaaS-Angebote und die dafür eingesetzten Rechenzentren so zu konfigurieren, dass die Kunden Wahlmöglichkeiten zwischen Jurisdiktionen und den entsprechenden Compliance-Standards haben.

4. Vertragstypologie

4.1. Generalunternehmermodell

Bild 3

Die Vertragstypologie des Cloud Computing folgt grundsätzlich den im traditionellen Outsourcing gängigen Strukturen (Bild 3). Die Bündelung verschiedener Anbieter sich gegenseitig ergänzender IT-Leistungen lässt sich vertraglich entweder durch ein Generalunternehmer-Subunternehmer-Verhältnis oder – bei „Überspringen" der Ebene des Generalunternehmers – im Rahmen einer Multi-Sourcing-Strategie des Kunden durch Einzelvertragsmanagement umsetzen. Tritt beim Cloud Computing ein einziger Dienstleister auf, der Rechenleistungen bündelt, die er über eigene Rechenzentren und/oder im Rückgriff auf Leistungskapazitäten Dritter vor-

hält, so steht er vertragsrechtlich als Generalunternehmer in vollem Umfang für die Leistungsfähigkeit und Leistungen sämtlicher Subunternehmer als Erfüllungsgehilfen im Sinne des § 278 BGB ein. In dieser Konstellation muss allein der Cloud-Anbieter die (gleichartigen oder sich komplementär ergänzenden) Leistungen seiner Subunternehmer koordinieren, abgrenzen und die Risiken der Zusage einer einheitlichen Gesamtleistung gegenüber dem Endkunden bewerten und absichern. Da der einzelne Subunternehmer in der Cloud üblicherweise keinen Einblick in Einzelheiten des Leistungsversprechens des Cloud-Anbieters gegenüber dem Endkunden hat, wird er sein Ausfallrisiko in der Regel standardisiert begrenzen und dementsprechend statische Haftungsbeschränkungen durchsetzen wollen. Soweit die Absicherung der Verfügbarkeit von Leistungen an herkömmliche Service Level Agreements und zugehörige Pönalen geknüpft wird, gerät der Subunternehmer schnell an die Grenze einer von seinem Geschäftsmodell nicht mehr abgedeckten Risikoverschiebung zu seinen Lasten. Angesichts On-demand-basierter Abrechnungsmodelle stehen Cloud Computing Anbieter vor der besonderen Herausforderung, ihre dauerhafte Leistungsbereitschaft trotz des womöglich ungewissen Abrechnungsvolumens attraktiv zu bepreisen. In diesem Spannungsfeld stellt eine übermäßige Verlagerung der Kosten und Haftungsrisiken von Leistungsausfällen auf den (bzw. die) Subunternehmer das Geschäftsmodell des Cloud Computing – gerade angesichts der Vielzahl von Übergabepunkten in der vernetzten Cloud – in wirtschaftlicher und vertragsrechtlicher Hinsicht auf die Probe.

Je internationaler das Netz der an einem Angebot beteiligten Rechenzentren, umso komplexer wird es damit zugleich, insbesondere im Rahmen der „Public Cloud“ durch einzelvertragliche Abreden ein ausgeglichenes Haftungsniveau zwischen dem Generalunternehmer und seinen Subunternehmern sowie innerhalb der ggf. nachgelagerten weiteren Subunternehmerkette sicherzustellen.

4.2. Leistungsabgrenzungen beim Multi-Sourcing

Bezieht der Kunde Cloud basierte Leistungen auf der Grundlage einer Multi-Sourcing-Strategie und stellt er (ggf. aus einer Plattform) eine Vielzahl von Einzelleistungen unterschiedlicher Anbieter selbst zusammen, so muss er sich im Rahmen des Vertrags- und Risikomanagements naturgemäß mit einer Vielzahl von Vertragsbedingungen und anwendbaren Rechtsordnungen auseinandersetzen. Im Zentrum der Vertragsgestaltung müssen dabei eine klare Leistungsabgrenzung und Definition der Übergabepunkte zwischen den Anbietern sowie die allgemeine Risikoabsicherung durch koordinierte Haftungsbeschränkungen stehen. Im Falle des Bezugs von Leistungen über eine Sourcing-Plattform stellt sich überdies die Frage nach der Haftung des Plattformbetreibers, der die Cloud bzw. die Einzelleistungen der verschiedenen Anbieter für die Kunden aufrufbar macht, für etwaige Fehlinformationen über Einzelangebote oder den Ausfall von Einzelleistungen, etwa durch Leitungsunterbrechungen beim Plattformzugriff.

4.3. ABG-rechtliche Einordnungen

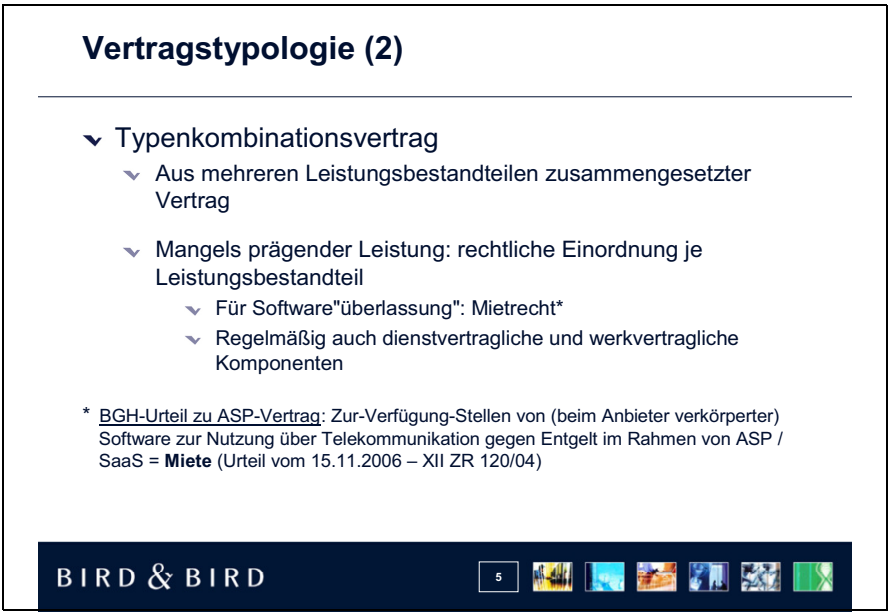


Bild 4

Die vertragstypologische Einordnung von IT-Dienstleistungen, denen ein On-demand-Abrechnungsmodell zugrunde liegt, wirft je nach Art und Nutzung der bereitgestellten Leistung weitere Fragen auf (Bild 4). Zwar ist die Bereitstellung virtualisierter Software im Rahmen von SaaS-Modellen typischerweise als Leistungsbeziehung mit mietähnlichem Charakter einzustufen und damit an die Rechtsprechung zum Application Service Providing anzuknüpfen[4]. Daraus folgt im Grundsatz eine Pflicht zur ständigen Erhaltung der bereitgestellten Software in einem für die vertragsgemäße Nutzung geeigneten Zustand, also eine kontinuierliche Pflicht zur Einpflegung von Software-Patches und anderen Maßnahmen der Fehlerbehebung. Werden allerdings Software-Applikationen zum Download auf die Systeme des Kunden bereitgehalten, so kann der Zugriff hierauf als eine Serie punktueller, im Rahmen des On-demand-Abrechnungsmodus' gegen Einmalgebühr erbrachter Einzelleistungen verstanden werden und können einzelne Elemente von Cloud Angeboten möglicherweise nach den Regeln über den Softwarekauf (mit entsprechend zeitlich beschränkbaren Gewährleistungspflichten) zu beurteilen sein.

[4] Maßgeblich ist hier das Urteil des Bundesgerichtshofs vom 15. November 2006 – XII ZR 120/04.

Kommt es zu einer Gemengelage von verschiedenartigen Leistungen und damit zu Typenmischverträgen, kann die Schwierigkeit einer eindeutigen vertragstypologischen Einordnung zu rechtlichen Unsicherheiten auch hinsichtlich der AGB-rechtlichen Zulässigkeit von Haftungsbeschränkungen und anderen Standardvertragsklauseln des Anbieters führen, da sich das AGB-Recht an der im BGB vorgegebenen Vertragstypologie orientiert. Insbesondere bei IaaS- und PaaS-Leistungen ist fraglich, ob kombinierte Angebote aus Netzleitungsdiensten und softwarebasierten IT-Dienstleistungen als reine Dienstverträge oder als mietähnliche Rechtsverhältnisse zu verstehen sind, wobei bei Annahme eines rein dienstvertraglichen Charakters die gesetzlichen Einstands- und Gewährleistungspflichten weitaus geringer wären als bei Annahme eines Mietvertrages.

5. Urheberrechtliche Fragen

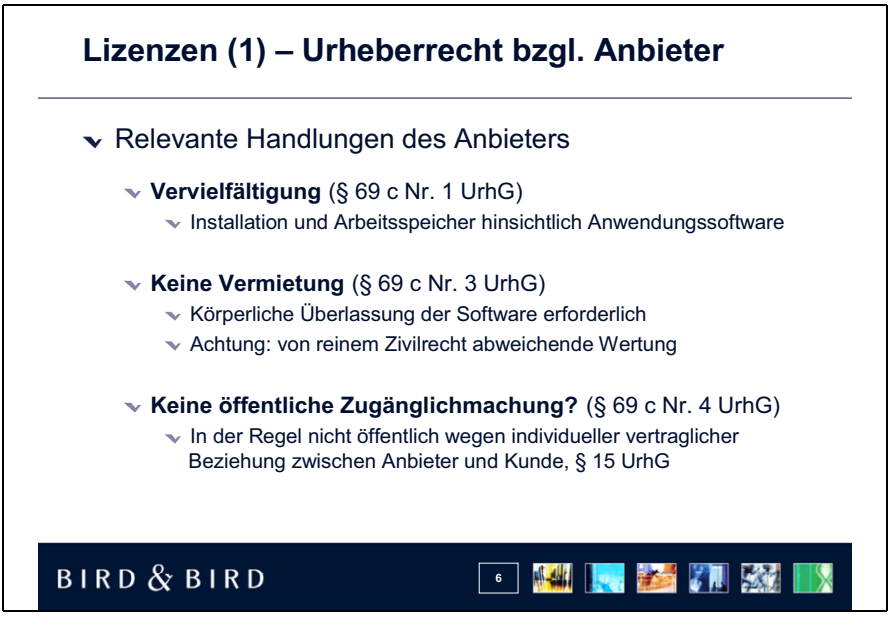


Bild 5

Auf Anbieter- und auf Kundenseite sind vor allem beim SaaS einige urheberrechtlichen Fragen näher zu betrachten (Bild 5). Der Anbieter von SaaS vervielfältigt die angebotene Anwendungssoftware, indem er ein Werkstück der Software auf einem Server installiert und für den Nutzerzugriff bereithält. Abweichend von einer rein zivilrechtlichen Bewertung erfolgt dabei im urheberrechtlichen Sinne keine „Vermietung" der Software an den Kunden (gemäß § 69 c Nr. 3 UrhG), solange es zu keiner Überlassung eines Werkstücks der Software in verkörperter Form kommt, wie dies etwa bei einem Download oder einem Laden der Software in den Arbeits-

speicher des Kunden der Fall wäre.[5] Ebenso wenig findet in aller Regel eine öffentliche Zugänglichmachung der Software im Sinne des § 69 c Nr. 4 UrhG statt, da die Software typischerweise aufgrund einer individuellen vertraglichen Beziehung gerade für den Kunden und nicht für die Öffentlichkeit bereitgestellt wird (siehe § 15 UrhG). Je nach technischer Ausgestaltung der Verfügbarmachung im Einzelfall sind abweichende Bewertungen jedoch denkbar.

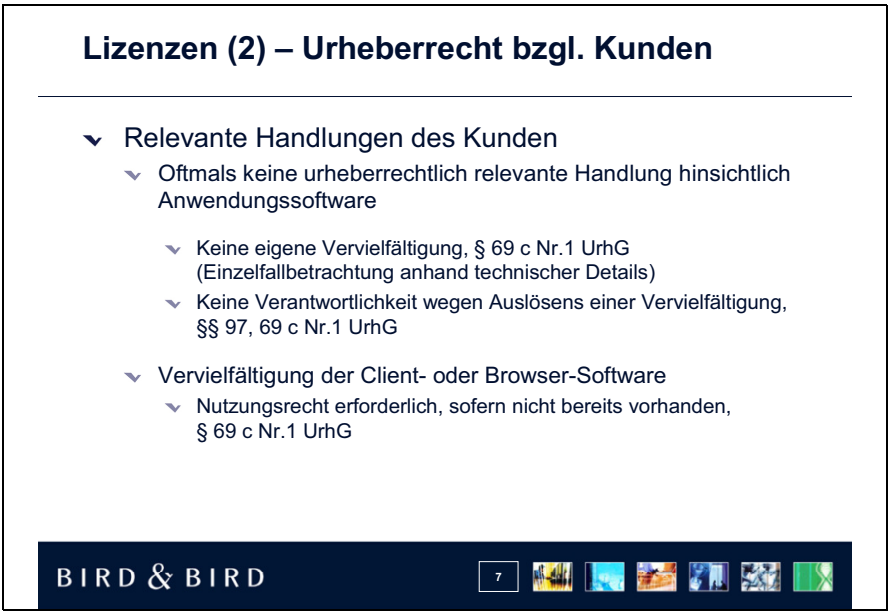


Bild 6

Erhebliche Bedeutung hat nach der bisherigen urheberrechtlichen Lehre die Grenzziehung zwischen einer rein browserbasierten Nutzung der Funktionalitäten einer Software einerseits und der Übertragung einer Kopie der Software in den Arbeitsspeicher oder auf die Festplatte des Kunden andererseits (Bild 6). Im letzteren Falle ist nicht nur eine urheberrechtliche Nutzungsrechtseinräumung an den Kunden erforderlich, sondern es können sich auch die vorwiegend im Kontext des Gebrauchtsoftwarehandels diskutierten und bislang nicht höchstrichterlich entschiedenen Fragen der „Erschöpfung" des urheberrechtlichen Verbreitungsrechts an im Wege des Online-Vertriebs überlassenen Softwarekopien stellen.

Unter der Annahme, dass der reine Browserzugriff auf eine im Rahmen des Cloud Computing als SaaS bereitgehaltene Software mangels Downloads keine Verviel-

[5] Maßgeblich ist insoweit, dass das Computerprogramm auf einem körperlichen bzw. elektronischen Datenträger – ggf. wie beim Arbeitsspeicher auch nur zeitlich begrenzt – abgelegt wird.

fältigung des betreffenden Werkstücks beim Kunden auslöst, entfällt damit ein urheberrechtlich relevanter Nutzungs- bzw. Lizenzierungsvorgang. In der Konsequenz würde sich die von ihm gezahlte Vergütung als Entgelt für eine reine Dienstleistung darstellen. Ob sich diese Schlussfolgerung bei vertiefter Betrachtung der technischen Gegebenheiten generell durchsetzen wird, ist mangels klarer Rechtsprechung zur urheberrechtlichen Bewertung von Browserzugriffen im deutschen Recht noch nicht abzusehen.[6] Eine Einzelfallbetrachtung anhand der technischen Einzelheiten ist in jedem Fall unerlässlich. Bei der Vertragsgestaltung wird man auf Anbieter- und Kundenseite gut daran tun, für SaaS Angebote die urheberrechtlichen Nutzungsfragen – wenn auch nur rein vorsorglich – zu regeln.

6. Datenschutz und IT-Sicherheit

Bild 7

Angesichts der weltweiten und hoch komplexen Verknüpfung von Rechenleistungen wird – über das bereits im Rahmen des „klassischen" IT-Outsourcing hohe Absicherungsbedürfnis hinaus – die Umsetzung der regulatorischen Anforderungen an Datenschutz und Datensicherheit zur zentralen Herausforderung des Cloud Com-

[6] Die jüngsten Entscheidungen des BGH vom 22. April 2009 zu „Internet-Videorecordern" (I ZR 215/06; I ZR 175/07; I ZR 216/06) weisen hier zumindest insofern den Weg, als dass der BGH auf die genauen technischen Abläufe abstellt, um ggf. einen Vervielfältigungsvorgang festzustellen.

puting (Bild 7). Der rasante Anstieg des öffentlichen Bewusstseins und der Anforderungen von Kunden, Gesetzgeber, Aufsichtsbehörden und Gerichten – nicht zuletzt des Bundesverfassungsgerichts mit seinen Entscheidungen zur Vorratsdatenspeicherung – sind hier wegweisend.

6.1. Cloud Computing und Auftragsdatenverarbeitung

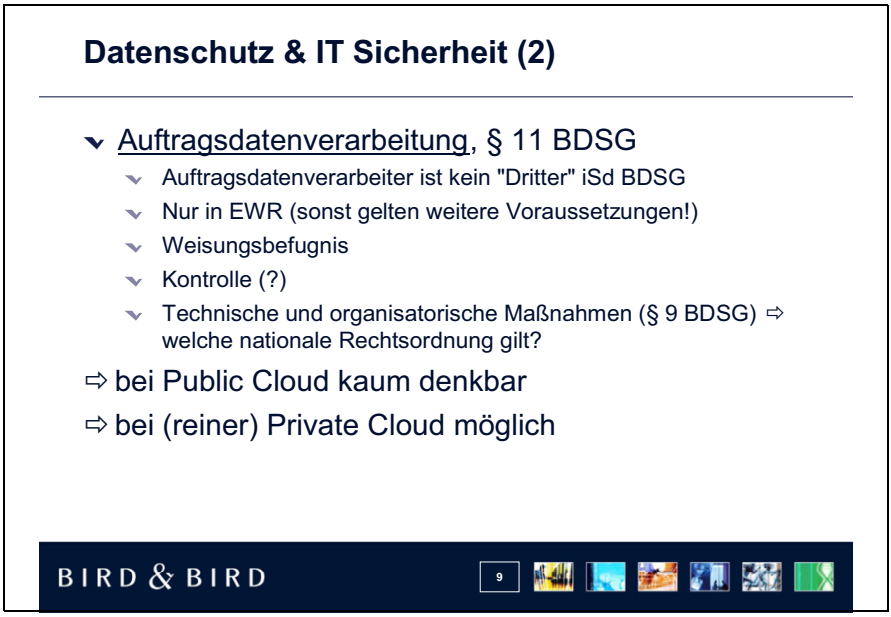


Bild 8

Zwar scheint das vom Bundesdatenschutzgesetz (BDSG) zur Verfügung gestellte Instrumentarium der Auftragsdatenverarbeitung im Prinzip geeignet, die weisungsgebundene Verarbeitung von personenbezogenen Daten abzusichern, die ein (gewerblicher) Kunde einem Cloud-Dienstleister zur Verfügung stellt (Bild 8). Die seit der Gesetzesnovelle vom September 2009 im § 11 BDSG ausdrücklich formulierten Maßstäbe erweisen sich bei näherer Betrachtung als im Rahmen des Cloud Computing nur begrenzt umsetzbar. So mögen zwar der Kunde als Auftraggeber und der Betreiber der Cloud als Auftragnehmer eine streng weisungsgebundene Auftragsdatenverarbeitung vertraglich vereinbaren. Die tatsächliche Umsetzung der geforderten Einzelmaßnahmen – insbesondere hinsichtlich der Aufsichts- und Kontrollbefugnisse des Kunden – ist in der Praxis jedoch kaum darstellbar. Bestenfalls im Rahmen einer Privaten Cloud kann man sich derzeit vorstellen, dass sich der Kunde die geforderten Kontrollmöglichkeiten nicht nur vertraglich vorbehält, sondern sie auch tatsächlich durchsetzen kann. Gemäß § 11 Abs. 2 Satz 4 BDSG hat sich der Auftraggeber „vor Beginn der Datenverarbeitung und sodann regelmäßig von

der Einhaltung der beim Auftraggeber getroffenen technischen und organisatorischen Maßnahmen zu überzeugen“ und ist „das Ergebnis zu dokumentieren“. Diese Anforderungen sind in der Cloud nur schwer oder gar nicht zu erfüllen. Zum einen sind die Leistungen und Infrastrukturzusammenhänge in der Cloud für den Kunden typischerweise nicht vollumfänglich transparent und sollen dies unter Umständen nach dem Willen des Anbieters auch nicht sein. Zum anderen sind eine hochkomplexe, multiple und ggf. mittels einer Vielzahl von Drittunternehmen zusammengesetzte IT-Infrastruktur sowie die zugehörigen Dienstleistungen und Softwareangebote möglicherweise nur sehr aufwändig zu dokumentieren, was aber gerade gemäß Datenschutzrecht erforderlich ist.

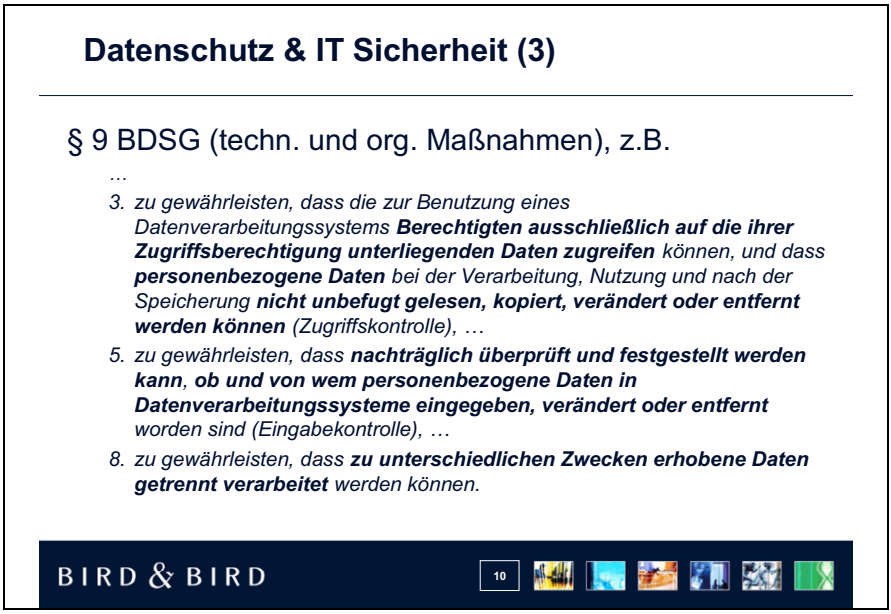


Bild 9

Darüber hinaus dürfte die Ausübung der gesetzlich geforderten Kontrolle sowohl für den Kunden als auch den Dienstleister mit erheblichen Kosten verbunden sein, die letztlich auf die mit dem Cloud Computing bezweckte Leistungsoptimierung und Kostenreduzierung durchschlagen (Bild 9). Insbesondere dürften in der Praxis ganz erhebliche Umsetzungsschwierigkeiten hinsichtlich der in § 11 Abs. 2 BDSG genannten Einzelmaßnahmen bestehen, wobei an dieser Stelle lediglich stichpunktartig auf § 11 Abs. 2 Nr. 3 (Dokumentation der technischen und organisatorischen Maßnahmen im Sinne des § 9 BDSG), Nr. 5 (Dokumentation der vom Auftraggeber vorzunehmenden Kontrollen), Nr. 6 (Berechtigung zu und Konkretisierung von Unterauftragsverhältnissen), Nr. 7 (Kontrollrechte des Auftraggebers und entsprechende Duldungs- und Mitwirkungspflichten des Mitauftraggebers) sowie Nr. 10

(Rückgabe überlassener Datenträger und Löschung beim Auftraggeber gespeicherter Daten nach Beendigung des Auftrages) verwiesen sein soll. Es bleibt abzuwarten, ob die Aufsichtsbehörden Leitlinien für die Auftragsdatenverarbeitung im Rahmen des Cloud Computing entwickeln.

6.2. Auskunftsrecht des Betroffenen

Bild 10

Ein weiterer wesentlicher – und in der Praxis kaum durchsetzbarer – Anspruch betrifft das Auskunftsrecht des Betroffenen (Bild 10). Gemäß § 34 BDSG hat jedes Individuum, dessen personenbezogene Daten verarbeitet werden, einen Auskunftsanspruch bzgl. Art und Umfang der gespeicherten Informationen. Die geschuldete Auskunft umfasst die Datenspeicherung und -verarbeitung durch den Anbieter und die von ihm einbezogenen Subunternehmer oder in sonstiger Weise einbezogenen Drittunternehmen und, damit verbunden, die Orte der Datenverarbeitung. Die Auskunft ist grundsätzlich unentgeltlich zu erteilen (siehe § 34 Abs. 5 BDSG). Für den Bereich der Public Cloud, die tendenziell eher den auf Einzelpersonen und Verbraucher ausgerichteten Cloud-Computing-Bedarf abdecken dürfte, wird man verstärkt über IT-Prozesse nachdenken müssen, die diesen Anforderungen bestmöglich entsprechen. Auch hier bleiben spezifische Äußerungen der Datenschutzbehörden abzuwarten.

6.3. Umsetzungsunterschiede innerhalb der EU

Der Blick auf die Umsetzung der EU-Datenschutzrichtlinien in die einzelnen nationalen Rechtsordnungen und die Verwaltungspraxis der Datenschutzbehörden innerhalb der EU zeigt gerade bei den Anforderungen an die technischen und organisatorischen Maßnahmen (siehe § 9 BDSG bzw. Artikel 2 b der Richtlinie 95/46/EG) und sonstiger Anforderungen an die Datensicherheit eine erhebliche Streuung sowohl der Regularien als auch der Durchsetzungspraxis. Es ist zu hoffen, dass sich die Arbeitsgruppe der nationalen Datenschutzaufsichtsbehörden der EU-Mitgliedsstaaten (die sog. Artikel 29 Gruppe) der Notwendigkeit vereinheitlichter Standards bewusst wird und gerade für das Cloud Computing und sonstige Formen international vernetzter Leistungsangebote eine Orientierungshilfe durch einen einheitlichen Mindeststandard technischer und organisatorischer Maßnahmen schafft. Derzeit führt die Disparität nationaler Anforderungen dazu, dass jedes in einer EU-Rechtsordnung ansässige Rechenzentrum im Rahmen seiner „Zulieferleistung in die Cloud“ zunächst den lokalen Anforderungen der für ihn maßgeblichen Jurisdiktion und ggf. den dazu ergangenen Ausführungsbestimmungen der Datenschutzaufsichtsbehörde zu folgen hat. Bei standardisierten Prozessen und entsprechenden Plattformangeboten ist abzusehen, dass dies erheblichen Aufwand für die Bewältigung entsprechender Komplexitäten auslöst.

6.4. Internationaler Datentransfer

Bild 11

Unterstellt man, dass Cloud-Computing nicht nur auf den Rechtskreis der EU und des ihm datenschutzrechtlich gleichgestellten Europäischen Wirtschaftsraums (EWR) beschränkt bleibt, so müssen sich Kunden und Anbieter des Cloud Computing mit der Frage des internationalen Datentransfers außerhalb der EU und des EWR in sog. „unsichere Drittländer" befassen (Bild 11). „Unsichere Drittländer" im datenschutzrechtlichen Sinne sind sämtliche Staaten außerhalb der EU und des EWR mit Ausnahme von Argentinien, Kanada, der Kanalinseln und der Schweiz, für die die EU ein adäquates Datenschutzniveau bestätigt hat. Das Haftungsprivileg des § 11 BDSG, durch das den Auftragsdatenverarbeiter für weisungsgebundene Datenverarbeitungsvorgänge keine eigenständige Haftung gegenüber dem Betroffenen trifft, greift nicht, wenn die Datenverarbeitung außerhalb der EU bzw. des EWR erfolgt. Anders als ein in der EU / dem EWR ansässiger Auftragsdatenverarbeiter ist ein Dienstleister in einem „unsicheren Drittland" datenschutzrechtlich stets als „Dritter" anzusehen (siehe § 3 Abs. 8 Satz 3 BDSG). Daraus folgt, dass für jeden Datentransfer an einen Dritten außerhalb der EU oder des EWR (sowohl an den primären Cloud-Dienstleister als auch innerhalb der Cloud an einen Subunternehmer) eine Datenübermittlung entweder aufgrund einer entsprechenden Einwilligung oder eines gesetzlichen Rechtfertigungstatbestands zulässig ist. Soweit eine sog. „informierte Einwilligung", die die ausdrückliche Benennung der Empfänger (also auch der einzelnen Subunternehmer und sonstigen Anbieter innerhalb der Cloud) voraussetzt, nicht eingeholt werden kann – wovon bei der Übermittlung von Kundendaten an einen IT-Dienstleister typischerweise auszugehen ist –, ist die Übermittlung ggf. durch einen der in § 4 c Abs. 1 BDSG genannten Tatbestände zu legitimieren[7], was jedoch erheblichen Begründungsaufwand auslösen kann. Darüber hinaus können Datentransfers an Drittunternehmen außerhalb der EU und des EWR datenschutzrechtlich nach Maßgabe der sog. EU-Standardvertragsklauseln (einschließlich derjenigen für Datenverarbeiter in Drittländern)[8] oder aufgrund verbindlicher Unternehmensrichtlinien (sog. Binding Corporate Rules) erfolgen (siehe § 4 c Absatz 2 BDSG). Allerdings bedarf ein Datentransfer, der nicht auf einen der Tatbestände des § 4 c Abs. 1 BDSG unmittelbar gestützt werden kann, im Sinne eines „Zwei-Stufen-Tests" zunächst einer materiellen Rechtfertigung z. B. im Sinne der §§ 28,29 BDSG, um sodann auf der Grundlage der EU-Standard-Vertragsklauseln abgesichert zu werden[9].

---

[7] § 4 c Abs. 1 Nr. 2 BDSG lässt Datentransfer zu, soweit dies „für die …. Erfüllung eines Vertrages zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist"; gemäß § 4 c Abs. 1 Nr. 3 ist die Übermittlung zulässig, soweit dies „…zum Abschluss oder zur Erfüllung eines Vertrages erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll."

[8] Die EU Kommission hat zum 5. Februar 2010 neue Standardvertragsklauseln für Datenverarbeiter in Drittländern bekannt gemacht (siehe Amtsblatt L 39 vom 12.02.2010, S. 5 ff.).

[9] Zur Begründung wird angeführt, dass anderenfalls der Datentransfer in ein unsicheres Drittland leichter durchführbar wäre, als dies für Datentransfers an Dritte innerhalb der EU / des EWR gelten würde, bei denen §§ 28, 29 BDSG oder andere gesetzliche Normen immer zu prüfen sind.

Dies stellt eine weitere beachtliche Herausforderung für die Anbieter von Cloud-Dienstleistungen dar, zumal in einzelnen EU-Jurisdiktionen solche Datentransfers auf der Grundlage der Standardvertragsklauseln einer gesonderten Vorlagepflicht bei den lokalen Datenschutzbehörden unterliegen können. Mit anderen Worten: Selbst wenn ein Datentransfer nach den Maßstäben deutschen Rechts gelingt, ist eine Weitergabe innerhalb der Cloud aus einem anderen EU-Staat z. B. in die USA oder nach Indien datenschutzrechtlich nicht notwendigerweise durch die Vereinbarung der EU-Standardvertragsklauseln zwischen Kunde und Anbieter (und zwischen Anbieter und seinen Subunternehmern) behördlicherseits vollständig abgesichert. Die Thematik ist der Anbieterseite im Wesentlichen bekannt und erfordert hohe Sorgfalt beim Zuschnitt entsprechender Cloud Computing Angebote. Zugleich drängt die Kundenseite zunehmend auf die detaillierte vertragliche Fixierung der vom Dienstleister vorgehaltenen IT-Infrastruktur einschließlich der Serverstandorte und der technischen Sicherungsmaßnahmen.

6.5. Branchenspezifische Besonderheiten

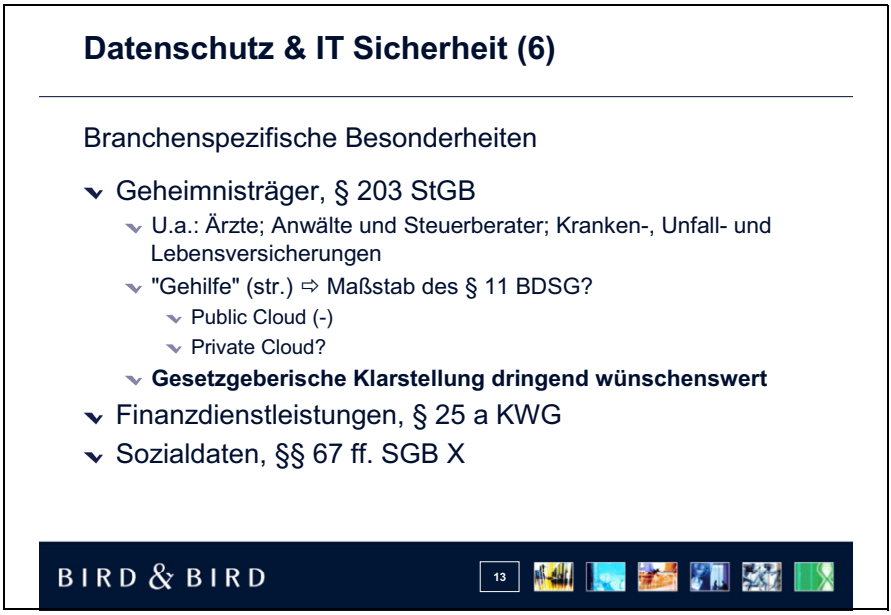


Bild 12

Über die allgemeinen regulatorischen Anforderungen an Datenschutz und Datensicherheit hinaus sind selbstverständlich auch im Rahmen des Cloud Computing branchenspezifische Anforderungen umzusetzen, wie dies z.B. für die Finanzdienstleistungsbranche aufgrund § 25 a KWG und der Regelungen der MaRisk etc. der Fall ist (Bild 12).

Eine besondere Hürde stellt für die Versicherungsbrache der § 203 Abs. 1 Nr. 6 Strafgesetzbuch (StGB) auf, der den Umgang von Geheimnisträgern mit den ihnen anvertrauten Geheimnissen betrifft und bei IT-Auslagerungen im Bereich der Kranken-, Unfall- oder Lebensversicherung problematisch wird. Es gehört zu den vieldiskutierten Fragen, ob und inwieweit durch Gesetzesauslegung und den Rückgriff auf die sog. „Gehilfenstellung" gemäß § 203 Abs. 3 Satz 2 StGB IT-Outsourcing an einen professionellen Dienstleister gerechtfertigt werden kann. In Ermangelung einer sehr wünschenswerten gesetzgeberischen Klarstellung wird man bei komplexen Dienstleistungsangeboten – und damit noch verstärkt angesichts der Komplexität des Cloud Computing – aus rechtlicher Sicht zu äußerster Vorsicht raten müssen, selbst wenn die vereinbarten und getroffenen Maßnahmen zur technischen Absicherung der Vertraulichkeit bzw. des Geheimnisschutzes den höchsten Anforderungen genügen.

6.6. Datensicherheit – der Umgang mit Sicherheitspannen

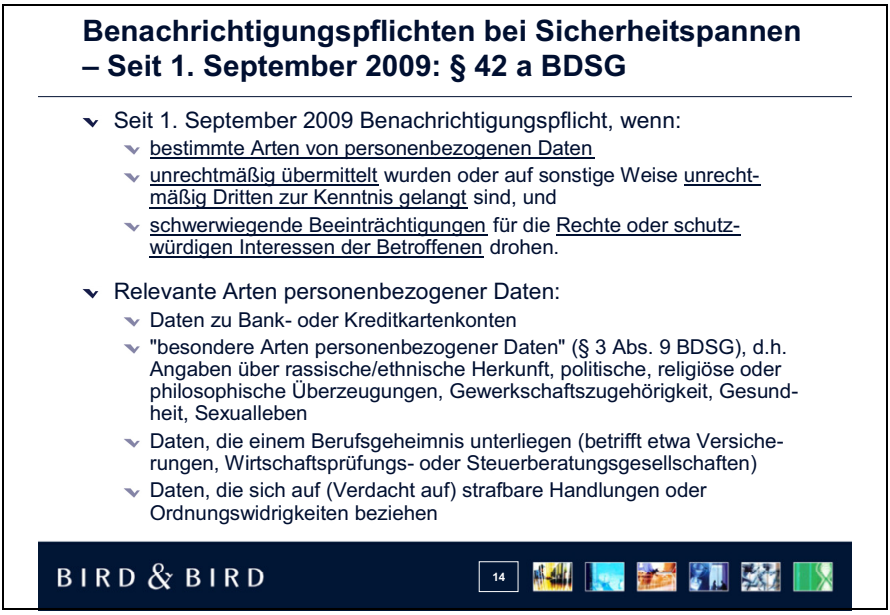


Bild 13

Im Zuge der Reform des BDSG vom 1. September 2009 hat der Gesetzgeber erstmals im neuen § 42 (a) BDSG – und parallel im § 15 (a) Telemediengesetz und § 93 Abs. 3 Telekommunikationsgesetz durch Verweis auf § 42 (a) BDSG – eine Regelung zum Umgang mit Datensicherheitspannen geschaffen (Bild 13). Danach ist die verantwortliche Stelle verpflichtet, bei unberechtigtem Zugriff Dritter sowohl die Aufsichtsbehörden als auch die Betroffenen zu informieren. Die Mitteilungspflicht

betrifft besonders sensible Daten, nämlich die sog. besonderen Arten von personenbezogenen Daten im Sinne des § 3 Abs. 9 BDSG (d. h. Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben), personenbezogene Daten, die einem Berufsgeheimnis unterliegen (dies betrifft insbesondere „Geheimnisse" im Sinne des § 203 StGB), Daten, die sich auf (den Verdacht von) strafbaren Handlungen oder Ordnungswidrigkeiten beziehen, sowie Bankdaten oder Daten über Kreditkartenkonten.

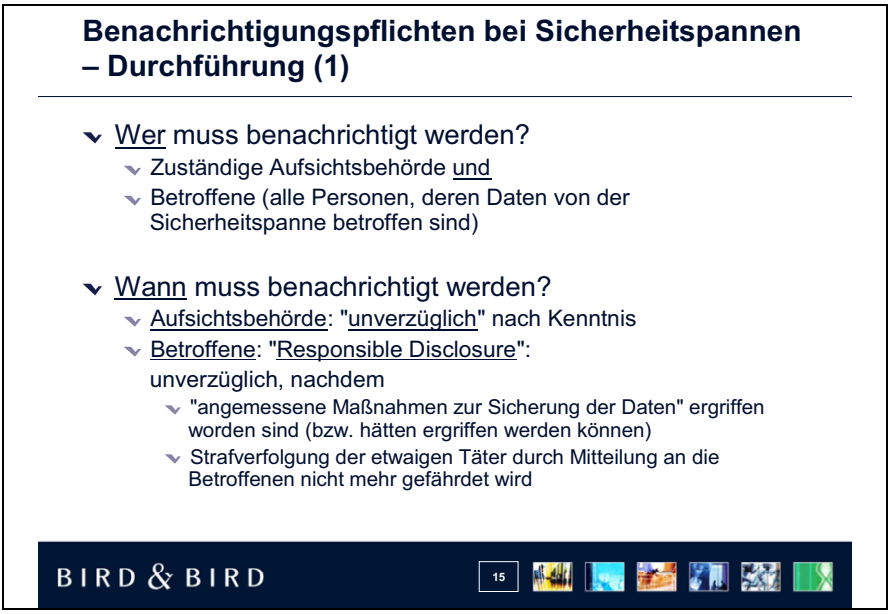


Bild 14

Die Benachrichtigungspflicht trifft in erster Hinsicht die verantwortliche Stelle, d. h. im gegebenen Kontext den Cloud-Kunden, der personenbezogene Daten in die Cloud gegeben hat. Zwar kann man gut vertretbar argumentieren, dass den IT-Dienstleister selbst keine Mitteilungspflicht trifft, wenn er mit dem Kunden eine Auftragsdatenverarbeitung wirksam vertraglich vereinbart hat[10] (Bild 14). Angesicht der für den Kunden in der Praxis jedoch kaum überschaubaren Datenverarbei-

[10] Die Bundesregierung ist nämlich im Rahmen des Gesetzgebungsverfahrens der Anregung des Bundesrates nicht gefolgt, die Benachrichtigungspflichten des § 42 (a) BDSG in den Katalog der Pflichten des Auftragsdatenverarbeiters gemäß § 11 Abs. 4 BDSG aufzunehmen (vgl. BT-Drucksache 16/12011, Anlage 3, S. 47). Vielmehr geht die Gesetzesbegründung offenbar von einer entsprechenden Mitteilungspflicht nur der jeweils verantwortlichen Stelle aus (vgl. BT-Drucksache 16/12011, S. 31 ff.).

tungsvorgänge in der Cloud, hat der Kunde aber in jedem Fall ein erhebliches Interesse daran, dem Cloud-Dienstleister vertraglich entsprechende Berichtspflichten aufzuerlegen, um seinen eigenen Pflichten gemäß § 42 a BDSG sowie ggf. den Sicherheitserwartungen seiner eigenen Kunden, deren personenbezogene Daten er verarbeitet, gerecht werden zu können. Es dürfte im Outsourcing und erst recht im Cloud Computing der gesetzgeberischen Zielsetzung zuwiderlaufen, wenn Datensicherheitspannen beim Dienstleister auftreten, der Kunde davon aber nur durch Zufall und jenseits eines kontrollierten Ablaufs erfährt und somit ggf. erst in einem viel späteren Stadium die Behörden und Betroffenen tatsächlich benachrichtigt werden.

Die Benachrichtigung selbst ist unverzüglich an die zuständige Aufsichtsbehörde sowie grundsätzlich auch individuell an jeden Betroffenen zu richten. Dabei gilt nach allgemeinem Verständnis gegenüber den Betroffenen das Prinzip des „responsible disclosure", d. h. die Mitteilung hat unverzüglich zu erfolgen, nachdem „angemessene Maßnahmen zur Sicherung der Daten" ergriffen worden sind (bzw. hätten ergriffen werden können) und/oder eine Strafverfolgung etwaiger Täter durch Mitteilung an die Betroffenen nicht mehr gefährdet werden wird.

Bild 15

Die Mitteilung gegenüber den Betroffenen muss dabei eine verständliche Art der Darstellung der Sicherheitspanne sowie empfohlene Maßnahmen zur Minderung nachteiliger Folgen enthalten, also z. B. bei einer Sicherheitspanne mit Kreditkar-

tendaten eine genaue Beschreibung des Vorfalls (Datum, Ort, Modalitäten der Sicherheitspanne) sowie die Empfehlung und genaue Angaben, über welche Kontaktdaten eine Sperrung der Kreditkartennummer zu veranlassen ist (Bild 15). Soweit die Mitteilung der Betroffenen (z. B. aufgrund des großen Kreises der Betroffenen) nicht möglich ist bzw. eine solche Mitteilung unverhältnismäßig aufwändig wäre, sieht das Gesetz alternativ und verpflichtend die Kollektivbenachrichtigung durch Anzeigen von mindestens einer halben Seite in mindestens zwei bundesweit erscheinenden Tageszeitungen oder „durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme“ vor. Zweifellos werden Datensicherheitsmaßnahmen und der Umgang damit in Zukunft ein deutlich höheres Maß öffentlicher Aufmerksamkeit erlangen. Kunden und Dienstleister müssen gleichermaßen ihre IT-Prozesse darauf ausrichten, Datensicherheitspannen zügig zu ermitteln und an das Krisenmanagement der verantwortlichen Stelle (also regelmäßig des Kunden) zu kommunizieren.

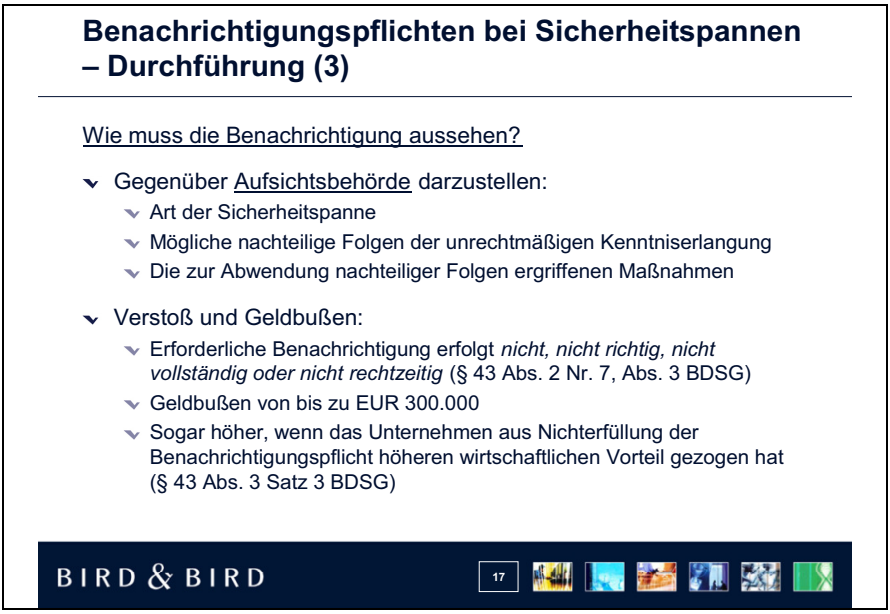


Bild 16

Der Gesetzgeber unterstreicht seine Anforderungen durch erhöhte Geldbußen von bis zu EUR 300.000, wenn die erforderliche Benachrichtigung nicht, nicht richtig oder nicht vollständig oder rechtzeitig erfolgt (siehe § 43 Abs. 2 Nr. 7, Abs. 3 BDSG) (Bild 16). Etwaige Bußgelder können jedoch auch höher ausfallen, wenn und soweit der wirtschaftliche Vorteil, den eine verantwortliche Stelle aus der betreffenden Ordnungswidrigkeit gezogen hat, den Betrag von EUR 300.000 überschreitet (siehe § 43 Abs. 3 BDSG).

7. Fazit

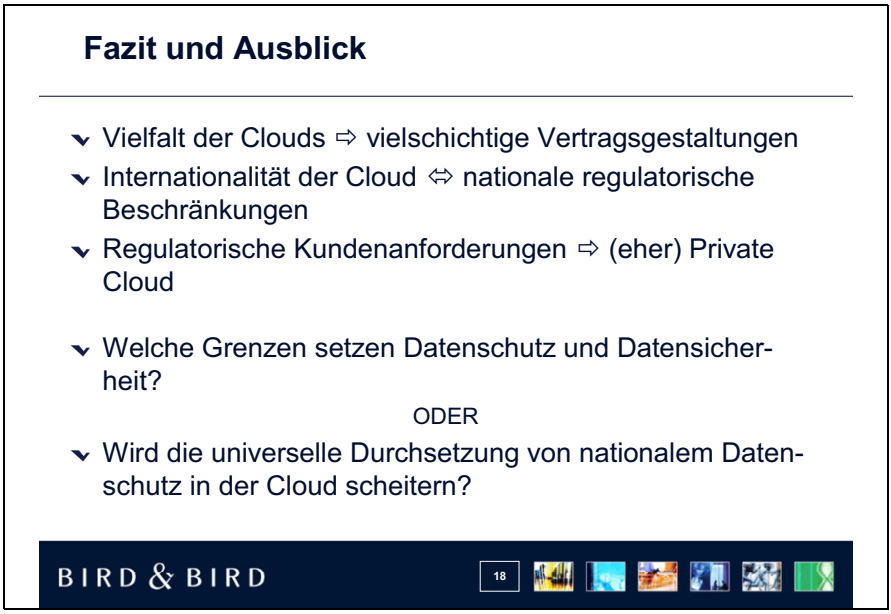


Bild 17

Im Ergebnis lässt sich festhalten, dass Cloud Computing als virtualisierte Form des IT-Outsourcing insbesondere in seiner internationalen Ausdehnung höhere Komplexität erzeugt als das „traditionelle Outsourcing“, die zusätzliche Anforderungen an die rechtliche Gestaltung und Absicherung durch Kunden und Anbieter stellt (Bild 17). Zwar lassen sich eine Vielzahl von Fragen auf die im traditionellen IT-Outsourcing entwickelten Lösungen zurückführen, die durch vertragliche Gestaltung insbesondere im Rahmen der Private Cloud und unter Berücksichtigung der spezifischen Kundenanforderungen umgesetzt werden können. Für die Bereiche Datenschutz und Datensicherheit ist jedoch fraglich, ob selbst bei sorgfältiger Konfiguration der zugrunde liegenden IT-Strukturen ein grenzenloses Cloud Computing zulässig ist: Sowohl die vertragliche Regelung der Auftragsdatenvereinbarung und der damit verbundenen Kontroll- und Aufsichtsrechte des Kunden als auch die Umsetzung des Auskunftsrechts des Betroffenen und der grenzüberschreitende Datentransfer aus der EU und dem Europäischen Wirtschaftsraum stoßen je nach konkreter Ausformung des Cloud Computing an rechtliche Grenzen. Für die Versicherungswirtschaft ergeben sich aus § 203 StGB zusätzliche rechtliche Unwägbarkeiten. Hier ist eine Klarstellung durch den Gesetzgeber wünschenswert, um durch Auferlegung strengster Anforderungen an Datenschutz und Datensicherheit die Kostenersparnisse durch IT-Outsourcing (einschließlich mittels Cloud Computing in der Private Cloud) – und damit auch den volkswirtschaftlichen Nutzen der Kos-

tensenkung im Gesundheitswesen – ohne rechtliche Kardinalrisiken für Kunden und Dienstleister zu ermöglichen. Ob und inwieweit darüber hinaus die Rechtsdurchsetzung des Datenschutzrechtes im Rahmen international aufgesetzten Cloud Computings – in der Private Cloud und erst recht in Public Clouds – vollumfänglich gelingen wird, ist angesichts der Divergenz regulatorischer Anforderungen im Einzelnen nach heutigem Stand zumindest eine offene Frage.

6 Technologien & Sicherheitsaspekte in Cloud Computing

Prof. Dr. Jörg Schwenk
Ruhr-Universität Bochum

Gestatten Sie mir zwei Anmerkungen zum Horst Görtz Institut vorweg, ein bisschen Eigenwerbung. Erste Anmerkung: Wir haben dieses Jahr die Ehre den 3. Deutschen IT Sicherheitspreis ausrichten zu dürfen, Preissumme 200.000 Euro, ausgeschrieben von der Horst Görtz Stiftung. Es würde mich freuen, wenn auch aus Ihrem Kreis Einreichungen kämen. Zweite Anmerkung: Unser Studiengang IT Sicherheit läuft jetzt seit fast 10 Jahren, und wir haben eine ganze Menge gute Absolventen. Im Mai ist die nächste Firmenkontaktbörse, wo Interessenten gern teilnehmen können.

Bild 1

Nun zum Thema: Technologien & Sicherheitsaspekte im Cloud Computing (Bild 1). Der Schwerpunkt meiner Ausführungen wird im Bereich Software as a Service liegen, also dieser flexiblen Cloud, und dort im Bereich Identitätsschutz. Mit diesem Thema beschäftigen wir uns in Bochum schon länger, auch aus juristischer Sicht. Ich werde versuchen durch ein Bild darzustellen, dass dieses Thema meiner Meinung nach immer wichtiger wird, wenn Sie Cloud Computing nutzen.

A. Picot et al. (eds.), *Trust in IT*, DOI 10.1007/978-3-642-18110-8_6,

Um ein aktuelles Beispiel zu zitieren und auch den Bogen zu einem Vorredner, Herrn Dr. Unkel von RWE, zu schlagen; es ging vor kurzem durch die Presse, dass ein Hacker sich Passwörter verschafft hat, um an eine Datenbank mit Emissionszertifikaten heranzukommen, und diese dann weiter verkauft hat. Es ist nicht so, dass die Hacker heute nur Online Banking attackieren. Die sind sehr kreativ. Wenn sie irgendwo Geld wittern, werden sie auch versuchen, dieses Geld zu bekommen. Wenn Ihre Daten bares Geld wert sind, müssen sie die schützen. Sonst kann es passieren, dass jemand darauf zugreift.

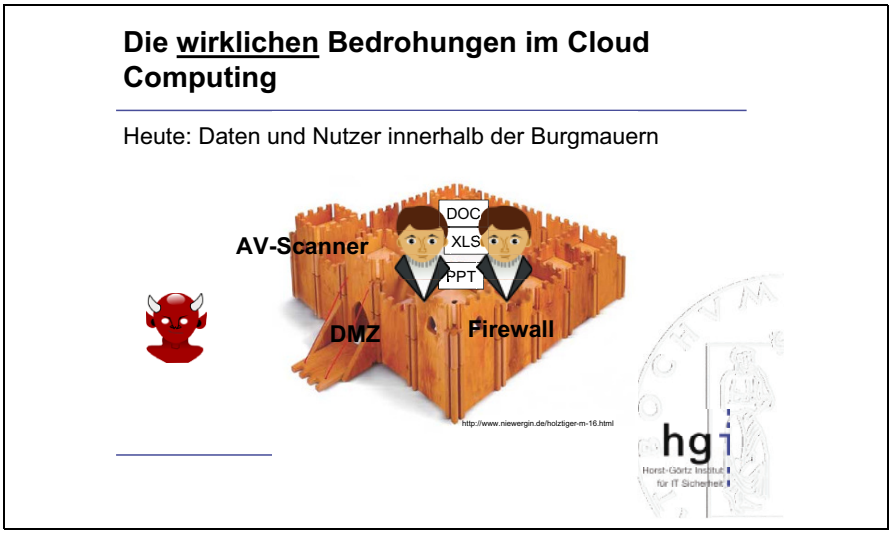


Bild 2

Ich will nicht in Abrede stellen, dass es viele andere Bedrohungen gibt, die man adressieren muss (Bild 2). Die Bedrohungen, die ich am interessantesten finde, ergeben sich aus folgender Überlegung, die ich hier grafisch dargestellt habe, vielleicht nicht dramatisch genug und noch zu verbessern. Wie ist es heute? Wenn Sie heute eine Firma betrachten, ein Intranet, dann sitzen die Nutzer meist zusammen mit den Daten in einer Art Festung, einer Art Burg. Sie haben rundherum Firewalls aufgebaut, wahrscheinlich einige Zugänge abgeschaltet, z.B. USB Zugänge zu den einzelnen Rechnern, damit nicht Daten unbegrenzt hinaus- und hineinwandern können. Sie haben Antivirenscanner, Sie haben eine demilitarisierte Zone. Was passiert heute, wenn Sie ein Problem mit Passwörtern haben? Das ist nicht so schlimm. Um an die Daten heranzukommen, muss man ja in die Burg rein. Also, wenn sie die Passwörter innerhalb der Burg verlieren, kann man das reparieren. Der Angreifer, das kleine Teufelchen sozusagen, sitzt außen und muss erst einmal die Burgmauern überwinden, bevor es die Passwörter nutzen kann. Zusammengefasst: Physikalischer Zugriff wird stark reglementiert, Firewalls, DMZ schützen, Antivirenscanner,

Intrusion Detection Systeme sind im Einsatz. Schwache Authentifikation reicht eigentlich, weil man noch andere Schutzmechanismen hat.

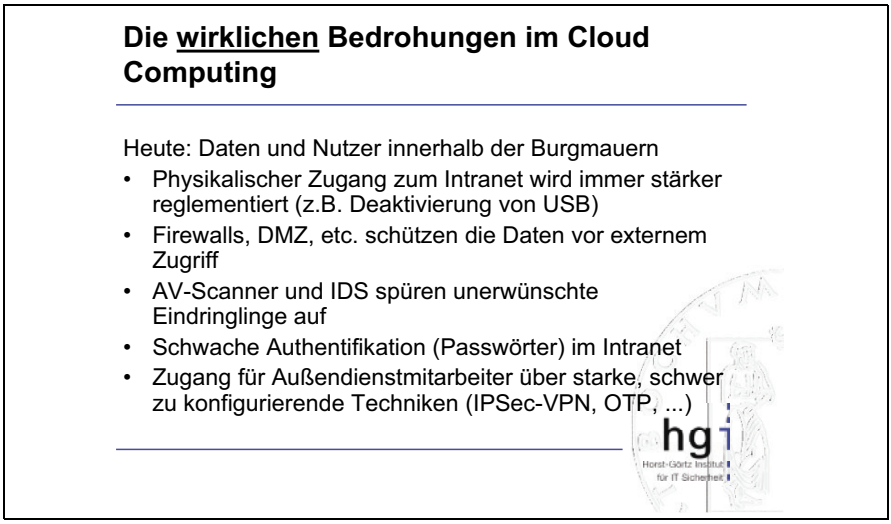


Bild 3

Außendienstmitarbeiter sind oft über starke Technologien und statische schwer zu konfigurierende Techniken eingebunden (Bild 3). Das würde den Bereich Infrastructure as a Service oder Plattform as a Service abdecken. Da könnte man ähnliche Techniken einsetzen.

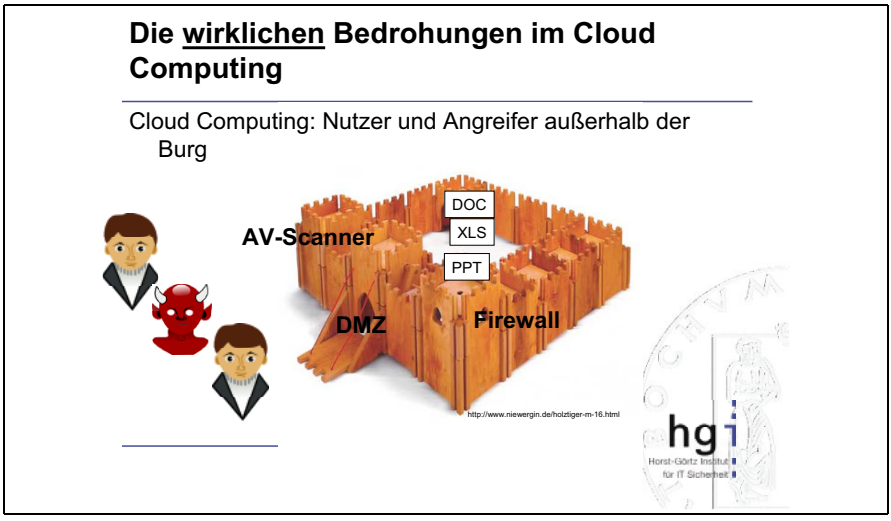


Bild 4

Bei Software as a Service ist das anders (Bild 4). Da sind Sie flexibler. Sie haben zwar die vertrauten Technologien alle noch, die im Rechenzentrum des Cloud Anbieters angewandt werden. Da gibt es demilitarisierte Zonen, Firewalls, Antivirenscanner, Intrusion Detection Systeme. Aber Sie sitzen jetzt außerhalb und sind als Nutzer nicht mehr in dieser Burg. Sie stehen praktisch auf einer Stufe mit dem Angreifer. Das ist das wirklich Neue beim Cloud Computing, und an dieser Stelle gibt es noch einige Probleme.

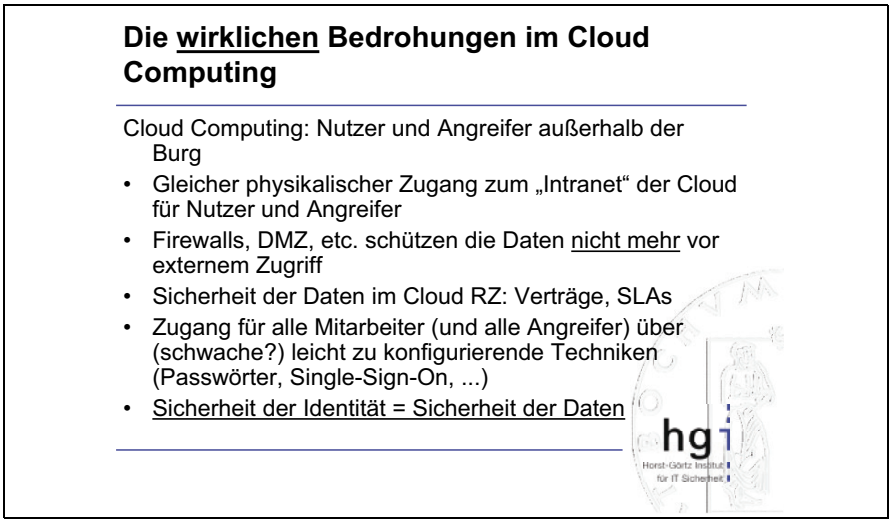


Bild 5

Hier vielleicht als Fazit (Bild 5): Es wird immer mehr so, dass die Sicherheit der Identitäten gleich der Sicherheit der Daten ist. Wenn Sie ein Problem mit Ihrem Identitätsmanagement haben, haben Sie ein Problem mit Ihren Daten. Ich werde das durch ein Beispiel untermauern. Wenn ein Angreifer also an Ihre Identitäten heran kommen, sind die Daten dem Angreifer preisgegeben, denn sie haben die gleiche Ausgangsposition.

Bild 6

Ich möchte jetzt näher auf zwei Aspekte eingehen (Bild 6). Zum einen ist das der Webbrowser, der oft als universelle Client-Software auch in der Cloud eingesetzt wird. Er kann sehr viel, hat auch Sicherheitsmechanismen, die aber noch nicht wirklich gut verstanden sind und nicht gut miteinander interagieren. Sie existieren so nebeneinander her, waren hervorragend für Web Shops geeignet, aber nicht wirklich für Hochsicherheitsanwendungen. Der zweite Schwerpunkt sind Web Services. Auch da gibt es noch große Probleme. Alle Probleme sind lösbar, werden aber im Moment noch nicht gelöst. Und darauf möchte ich hinweisen.

Der Webbrowser als universelle Client-Software.

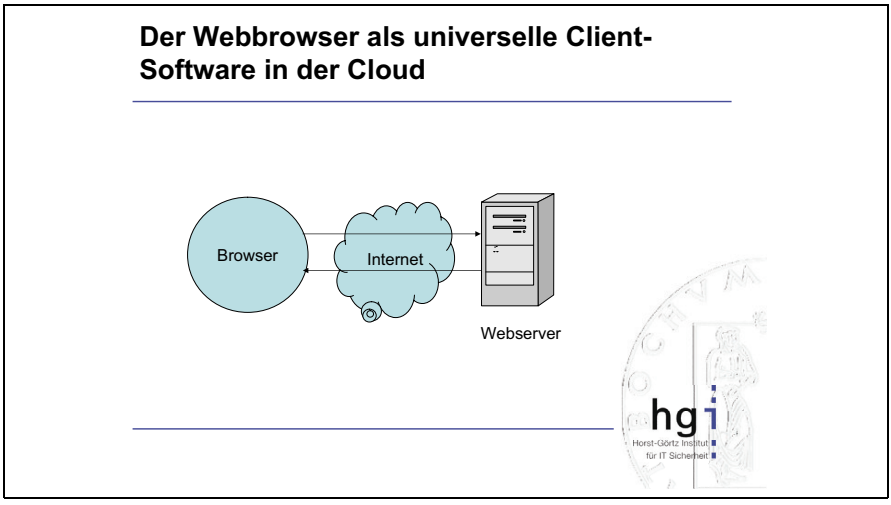


Bild 7

Die Situation früher: Ein Browser, der HTML beherrschte. Ein Webserver, der statische Seiten geladen hatte (Bild 7).

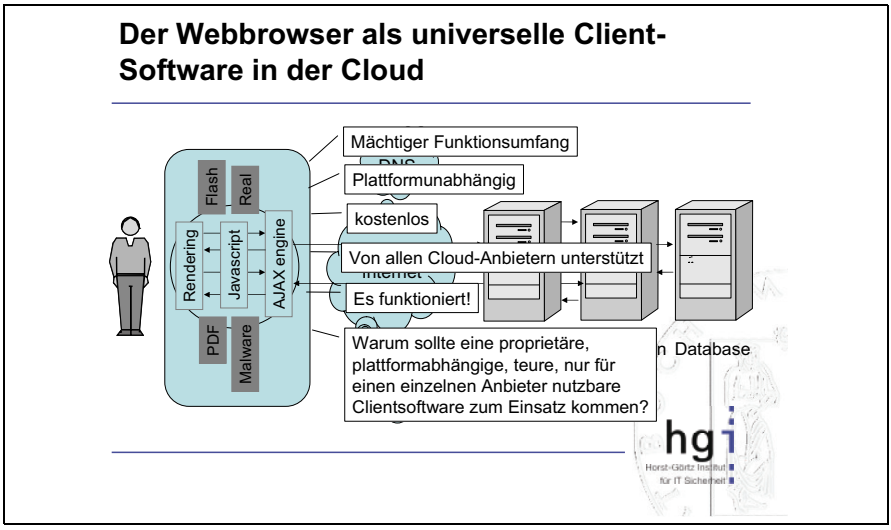


Bild 8

Heute sieht es ganz anders aus, und insbesondere der Browser ist mächtig aufgerüstet worden (Bild 8). Es gibt hier eine AJAX-Engine, die im Prinzip erst den Bedienkomfort bietet, so dass Sie mit dem Browser arbeiten können wie mit einer Desktopapplikation. Erst durch die AJAX-Engine wird es möglich, dass man wirklich Cloud Services, Software as a Service nutzen kann ohne Abstriche beim Komfort machen zu müssen. Es ist viel Javascript notwendig, was vielleicht auch ein Punkt beim Download von Software ist. [Anm. zum vorangegangen juristischen Vortrag.] Die Funktionalität des Browser wird ständig modifiziert und erweitert durch große Javascript-Bibliotheken. Man weiß nicht mehr so genau, was er überhaupt kann und was er nicht kann. Dazu kommen viele Plugins, die auch Probleme bieten. Es ist so, dass viele dieser Plugins, z.B. die Flash Plugins Funktionalitäten des Browsers duplizieren. Ein Angreifer kann sich jetzt aussuchen, was er angreifen will, einen Browser, ein Plugin? Fazit: der Browser bietet viele Angriffspunkte.

Im Bild hängen am Internet noch bewusst zwei Wolken, um auf deren Problematik hinzuweisen. Das Domain Name System und Public-Key-Infrastrukturen bilden die Basis für heutige Browsersicherheit. Heute wird allgemein verlangt, dass der Nutzer den Server identifizieren kann. Das soll man anhand des Domain Namens und eines passenden Zertifikats tun können. Ich denke, dass das immer noch problematisch ist, insbesondere bei großen Anwendungen, und ich möchte einfach als Denkanstoß hier mitgeben: Geht es nicht auch ohne? Es gibt Lösungen, die auch ohne das funktionieren, sowohl ohne DNS als auch ohne PKI.

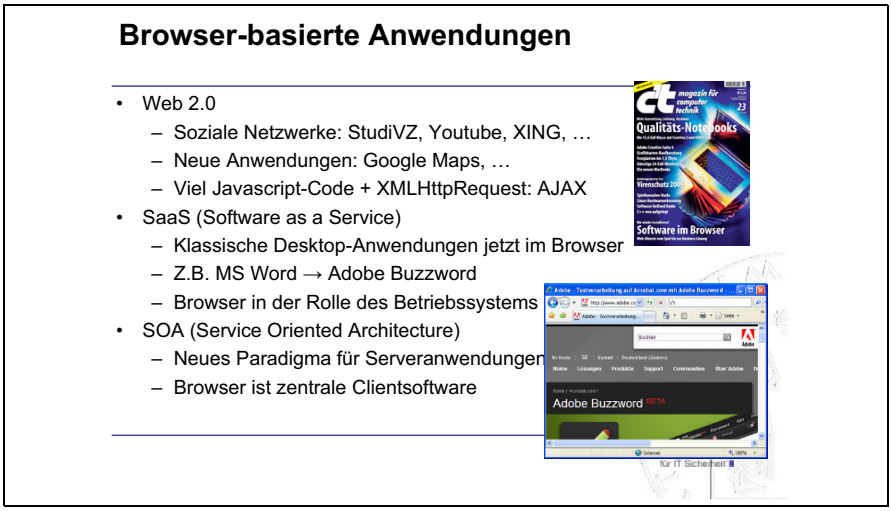


Bild 9

Warum ist der Browser so gut geeignet als universelle Clientsoftware (Bild 9)? Er hat einen sehr mächtigen Funktionsumfang. Er ist plattformunabhängig – Sie brauchen sich keine Gedanken über Ihre Plattform zu machen –, kostenlos und wird unterstützt. Die Protokolle sind gut verstanden. Es funktioniert einfach. Es gibt ganz viele Beispiele, bei denen es mit dieser Clientsoftware funktioniert. Warum sollte man dann eine proprietäre plattformabhängige Software entwickeln, wenn man das hat? Es ist eine ideale Wahl aus Sicht der Funktionalität.

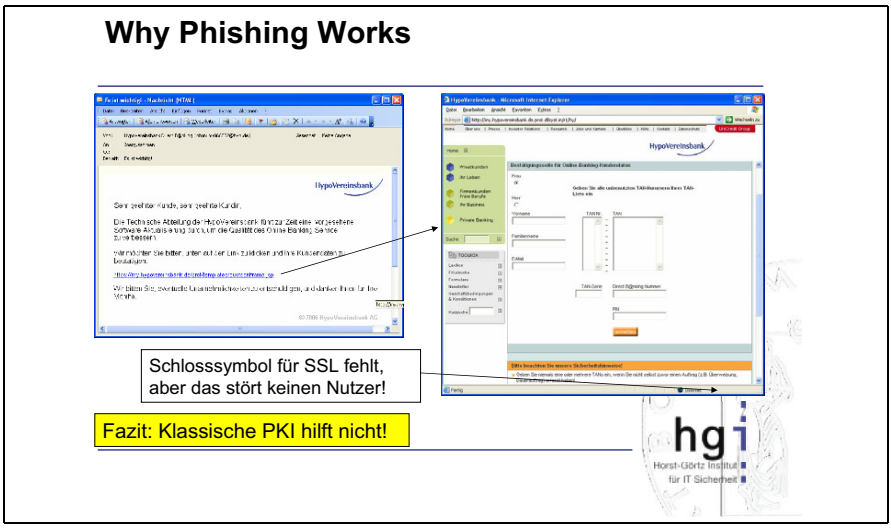


Bild 10

Aber er hat einige Probleme, was Ihnen sicher bekannt ist (Bild 10). Das Stichwort „Phishing“ ist jetzt schon sechs Jahre alt. 2004 fing es an, als man gemerkt hat, dass die SSL-Verschlüsselung und damit verbunden die Authentifikation des Webservers dem Nutzer nicht gut genug signalisiert wird. Bei den damaligen Browsern gab es nur ein winzig kleines Schlosssymbol ganz unten am Rand des Browsers. Heute ist es hoch gewandert in die Adressleiste. Es gibt auch diverse Farbcodes. Aber die große Schwachstelle ist immer noch, dass diese Farbcodes nicht konsequent umgesetzt sind: Man müsste eigentlich für unverschlüsselte Verbindungen den Farbcode rot verwenden und auf die Gefahr hinweisen. Aber es wird weiß genommen. Das heißt, der Unterschied zwischen unverschlüsselten und verschlüsselten Verbindungen ist einfach nicht da im Browser, und deswegen laufen die meisten Angriffe einfach ohne den Schutz durch SSL. Und der Nutzer merkt es nicht.

Es gibt auch spezielle Angriffstools, die das ausnutzen. Zum Beispiel gibt es ein Tool namens SSLStrip, das ausnutzt, dass ich eigentlich immer nur www.google.com eintippe und nie https://www.google.com. Dieses Tool macht immer eine unverschlüsselte Verbindung daraus. Auch solche Nutzerbesonderheiten werden ausgenutzt.

Klassische PKI hilft nicht wirklich. Sie bürden dem Nutzer eine Last auf, aber auch mit Extended Validation Zertifikaten ist es immer noch schwierig für den Nutzer, zwischen einem grünen EV-Zertifikat und gar keiner Verschlüsselung zu unterscheiden. Das ist einfach schwierig.

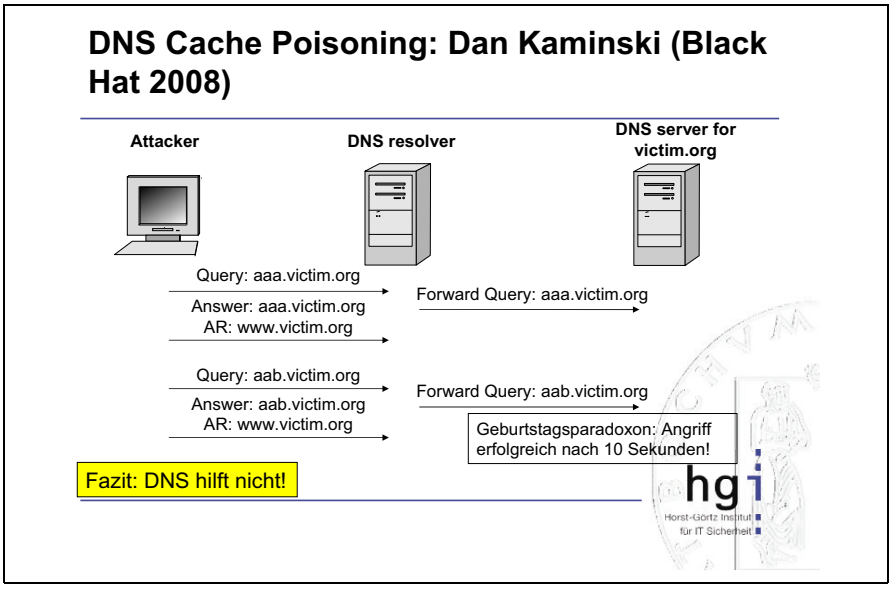


Bild 11

2008 war auch ein schwarzes Jahr für das Domain Name System. Dan Kaminski hat es eigentlich geknackt (Bild 11). Das Domain Name System ist tot. Man hat das Ganze gepatcht, indem man ein anderes Netzwerkprotokoll, nämlich UDP, dazu genommen hat. Also, innerhalb von DNS war das nicht zu reparieren. Man konnte innerhalb von 10 Sekunden jeden beliebigen Server „vergiften“ und falsche Angaben in den Cache reinschreiben. Damit hätten ein Angreifer beliebige Domain Namen auf einen von ihm kontrollierten Server umleiten können. Es ist noch gepatcht, aber wie gesagt, nicht innerhalb des Domain Name Systems sondern außerhalb.

Der nächste Angriff wird fatal. DNSSEC ist sehr komplex, riesengroß. Die Einführung braucht noch Zeit. Es ist die Frage, ob das hier helfen kann. An der Stelle würde ich mich erst einmal nicht auf das Domain Name System verlassen. Es fällt als Basis für Sicherheitsentscheidungen auch weg.

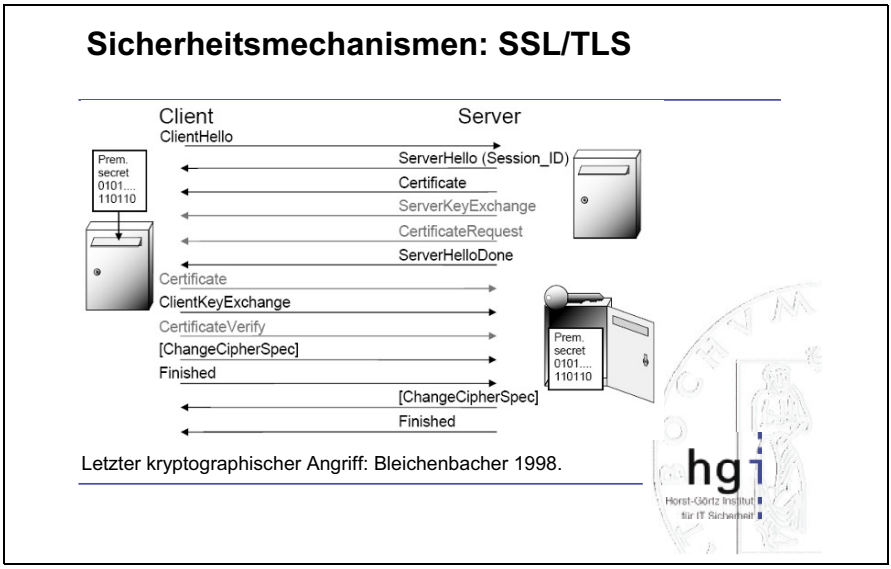


Bild 12

Was ist noch problematisch im Browser (Bild 12)? Der Browser hat ja zwei große Sicherheitskomponenten, das Secure Socket Layer (SSL) Protokoll, das eine verschlüsselte Verbindung zum Server aufbaut und die sogenannte Same Origin Policy.

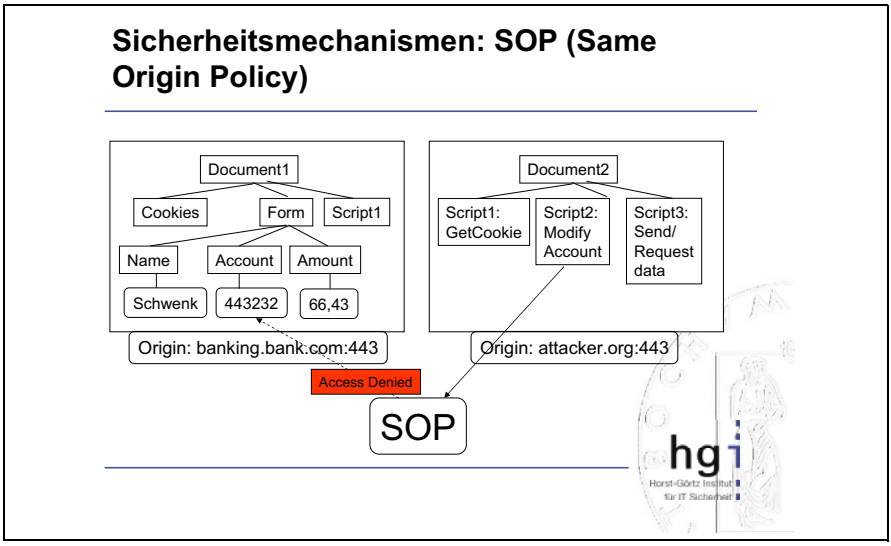


Bild 13

Die Same Origin Policy entscheidet, ob ein bestimmter Datensatz an bestimmte Server gesendet werden darf oder nicht (Bild 13). So sollen zum Beispiel Cookies immer nur an Server in der gleichen Domain zurückgesendet werden, von wo sie auch ausgesetzt wurden.

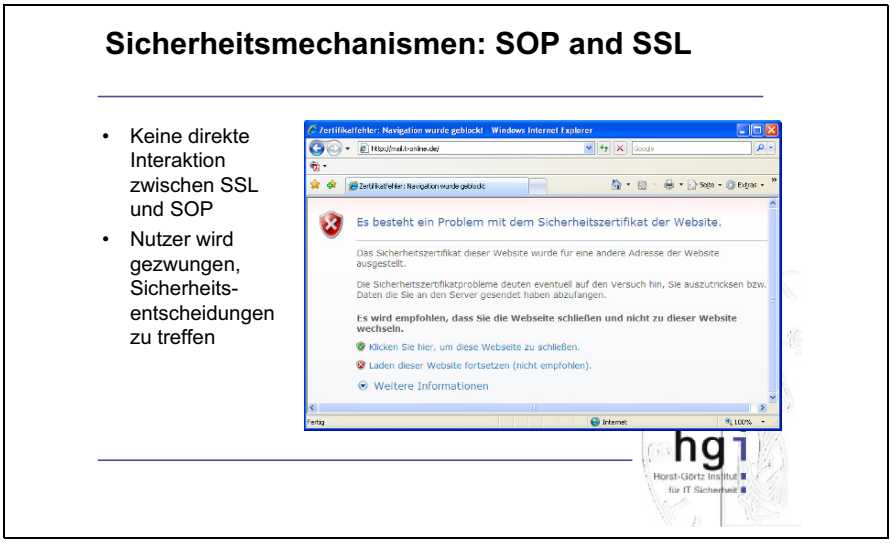


Bild 14

Was passiert, wenn es hier Probleme gibt? Das ist ein Fall, der gar nicht so selten auftritt. Sie treffen einfach auf eine Webseite und da gibt es Probleme mit dem Zertifikat (Bild 14). An der Stelle wird der Nutzer ins Spiel gebracht, der entscheiden muss, ob das vertrauenswürdig ist oder nicht. Man kennt das aus Studien, wenn der Nutzer ein Ziel erreichen möchte, irgendwohin möchte, klickt er diese Warnmeldung meistens weg. Danach verhält sich der Browser so, als hätte es gar kein Problem gegeben. Und das ist der Punkt. An dieser Stelle könnte der Browser ein bisschen mehr aufpassen. Wenn Sie zum Beispiel einen geheimen Wert im Cookie gespeichert haben und es tritt so ein Problem auf, dass der Nutzer wegklickt, dann verhält sich der Browser so, als gäbe es kein Problem und gibt das Geheimnis bereitwillig preis.

In Kombination mit diesen Angriffen auf das Domain Name System gab es noch 2008 einen Angriff auf Public Key Infrastrukturen. Kollisionen im MD5 Hashalgorithmus wurden ausgenutzt, und es wurden gefälschte (aber gültige!) Serverzertifikate ausgestellt. Da kommen eine Menge Probleme zusammen, diese Kombination aus Domain Name System und PKI ist problematisch.

Es gibt Lösungen, und man kommt davon weg. Aber später mehr dazu.

Bild 15

Ich komm zum zweiten Problemkreis und mute Ihnen ein bisschen XML Code zu, aber nur um zu verdeutlichen, dass es eine komplexe Datenstruktur ist, die noch nicht wirklich verstanden ist (Bild 15).

Bild 16

Das hier ist der Grundaufbau einer digitalen Signatur in XML (Bild 16). Die ist deutlich komplexer als eine digitale Signatur, wie Sie sie z.B. aus dem Signaturgesetz kennen, aus dem Email-Umfeld, denn hier wird zweimal gehasht bevor signiert wird. Das sind die beiden Pfeile 1 und 2. Was Sie machen müssen, ist, dass Sie zunächst dieses Referenzelement nehmen müssen. Da steht eine URI drin. Sie müssen sich die Daten holen und dürfen diese beliebigen Transformationen unterwerfen. Nach diesen Transformationen wird ein Hashwert gebildet, der erst einmal in die XML-Signatur hineingeschrieben wird. Dann wird noch einmal das ganze Element SignedInfo genommen, mindestens einer komplexen Transformation unterworfen, wieder gehasht und dann das Ganze erst mit dem Signaturwert verglichen.

Darauf sind viele Angriffe denkbar. Man kann zum Beispiel Transformationen ansetzen, die einfach immer alles auf das leere Dokument abbilden. Dann ist die Signatur für alle Dokumente gültig. Das ist mit diesem Standard möglich. Es ist nicht verboten, aber natürlich sinnlos, und man kann es bemerken.

Ich möchte auf einen Angriff hinaus, der jetzt seit fünf Jahren bekannt ist, aber nach meiner Schätzung in fast keinem kommerziellen Produkt wirklich berücksichtig wurde. Das sind die sogenannten XML Wrapping Attacken, die von Michael McIntosh und Paula Austel 2005 vorgestellt wurden. Sie beziehen sich auf einen

wichtigen Standard, auf WS Security. Mit diesem Standard sollen SOAP Nachrichten in ihrer Integrität geschützt werden. Die beiden konnten zeigen, dass das nicht der Fall ist. Die Integrität der Nachrichten ist nicht geschützt. Man kann sie beliebig ändern. Dieses Problem besteht weiterhin, und das gibt es heute noch in vielen Produkten.

Was kann man hier tun? Dieses Problem ist eine Besonderheit dieser XML Signatur. Bisher war es immer so, dass eine Applikation genau wusste, wo die zu signierenden Daten stehen. Wenn Sie eine signierte Email empfangen, weiß der Email Client, welche Daten er hashen muss und wo die Signatur steht. Bei XML Signaturen weiß das die Software nicht mehr, sondern die Software bekommt es durch den Datensatz selbst mitgeteilt. In diesem Datensatz steht der Verweis auf den Ort, an dem sich die signierten Daten befinden, ganz unten links, wenn sie den Pfad runtergehen. Und der WS Security Standard sagt jetzt, dass man dafür möglichst ein ID-Attribut nehmen sollte, das einen eindeutigen, im Dokument nur einmal vorkommenden String enthält. Hier heißt das String einfach „theBody“. Wenn die Nachricht abgesendet wird, sieht sie so aus wie hier. Dann steht im SOAP Body, wo die Daten stehen, id=“theBody“, rechts oben.

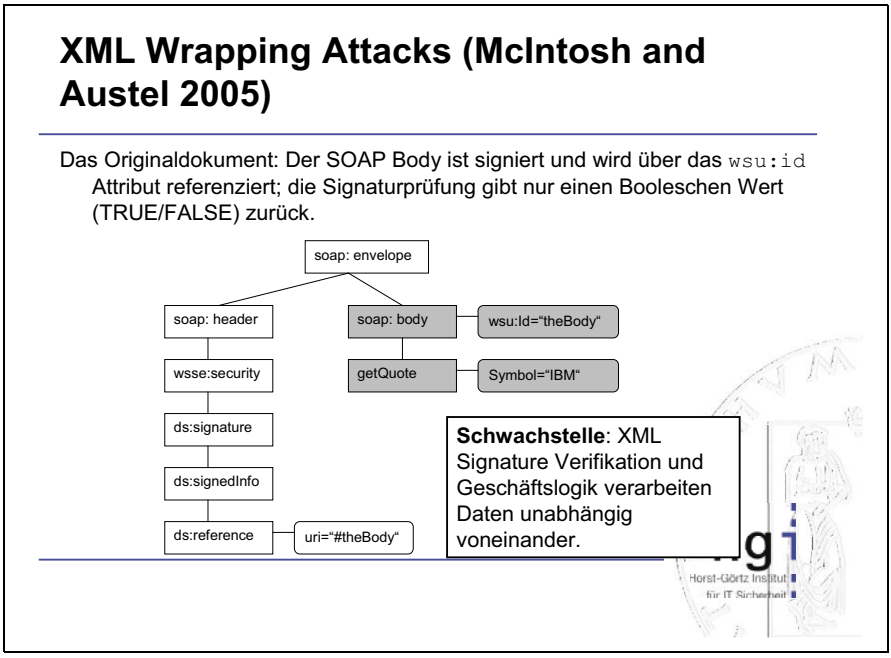


Bild 17

Was die beiden Autoren hier beobachtet haben, war zunächst einmal, dass die Signaturverifikation und die Verarbeitung der Daten unabhängig voneinander sind (Bild 17). Man kann diese signierten Daten einfach irgendwohin verschieben in diesem Dokument und in den Body unsignierte Daten schreiben. An dieser Stelle fängt jetzt die Verifikation an zu wirken. Wenn Sie diese Signatur verifizieren wollen, dann sagt der Standard „schauen Sie dann nach dem ID Attribut “theBody“, suchen Sie das irgendwo im XML Dokument“. Es wird gefunden, wird verifiziert und die Signaturverifikation liefert „ok“ zurück. Die Signatur ist gültig. Dann kommt die Applikationslogik und verarbeitet die Daten, aber sie nimmt die Daten aus dem Body und verarbeitet sie. Damit haben Sie ungültige Daten eingeschleust, und die werden auch verarbeitet.

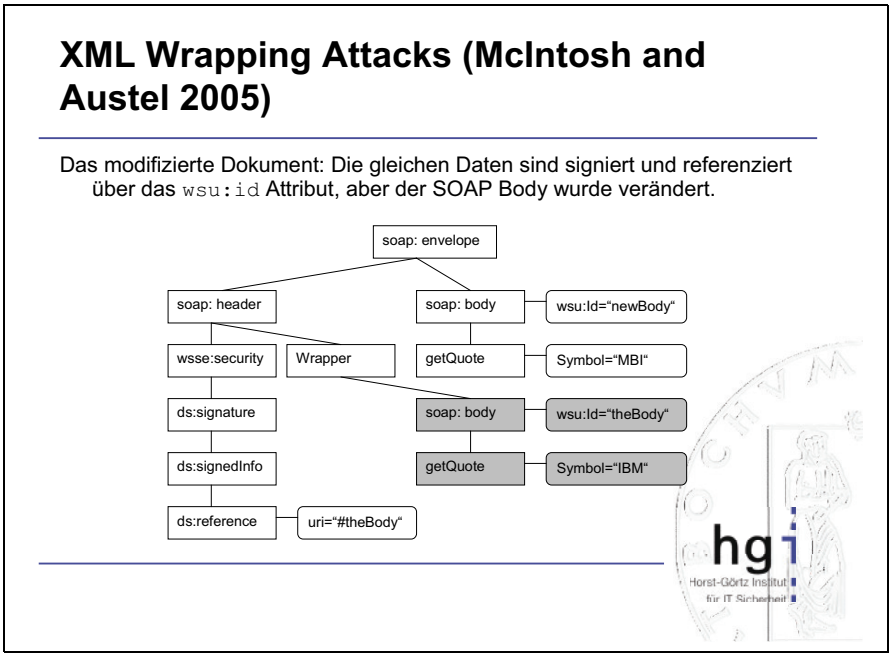


Bild 18

Um die Beziehung zur Cloud noch deutlicher zu machen, gibt es noch eine nette Variante dieses Angriffs, die etwas anders funktioniert (Bild 18). Sie wurde von zwei Kollegen bei NEC in Heidelberg gefunden und bezieht sich auf die Amazon Cloud. Es gab ein echtes Problem in der Amazon Cloud, das mittlerweile behoben ist. Auch da ging es wieder um diese ID Attribute. Vorher noch etwas anderes.

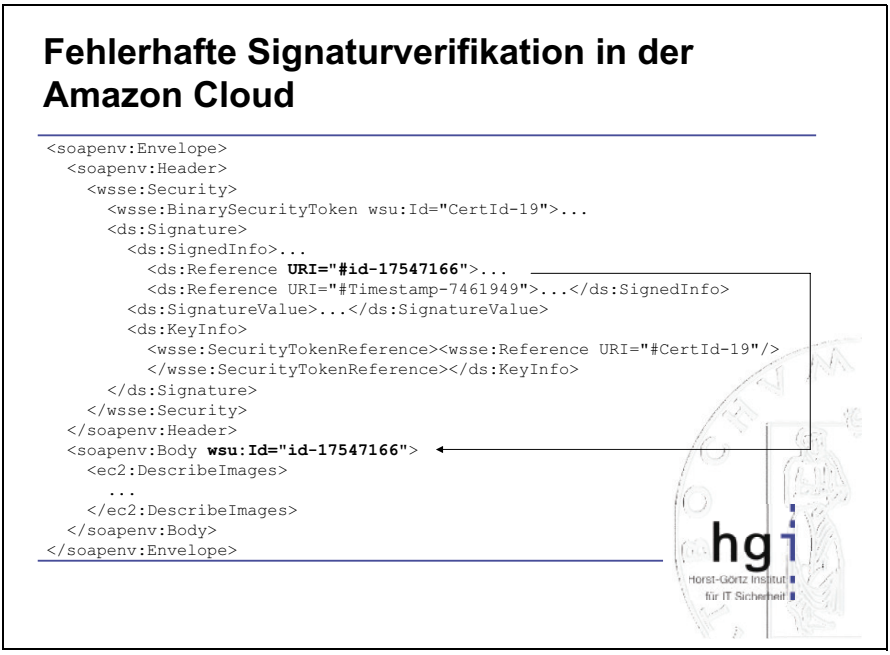


Bild 19

Es gibt diese Referenz, fett hervorgehoben, diese Verlinkung zwischen der Referenz und den signierten Daten (Bild 19). Die beiden, Nils Gruschka und Luigi Lo Iacono, haben folgendes gemacht. Sie haben vor die eigentlichen Daten einen zweiten Datensatz geschoben mit genau der gleichen ID, und der macht etwas völlig anderes in der Cloud. Die eigentlichen Daten sagen DescribeImages, also liefern nur Daten zurück und der gefälschte Datensatz macht ein RunImage, startet einen neuen Prozess. Was ist damals passiert? Es gab wieder eine unterschiedliche Auswertung der Datensätze bei der Verarbeitung und bei der Signaturverifikation. Die Signaturverifikation verläuft nach dem Paradigma DOM. Hier werden diese einzelnen Elemente in Objekte geladen, und diese Objekte werden verarbeitet.

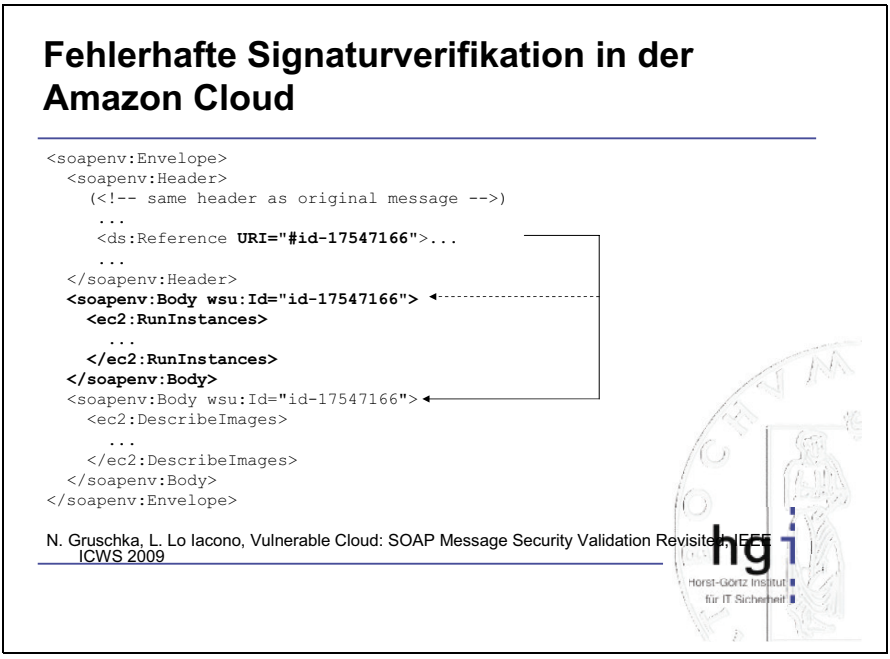
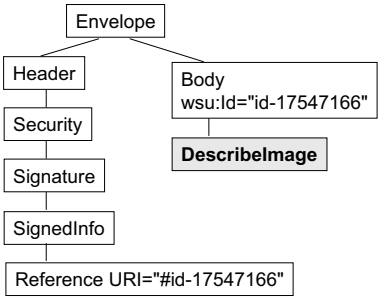


Bild 20

Bei der Signaturverifikation passiert Folgendes (Bild 20): Es wird zunächst einmal dieses fett gedruckte Element mit der ID geladen, dann aber von dem echten Element überschrieben, weil es die gleiche ID hat. Das heißt, im Speicher steht der korrekte Datensatz, gegen den die Signatur überprüft wird, und die Verifikation liefert ein „ok“ zurück. Wenn jetzt aber die Datenverarbeitung kommt und die Daten ausführen soll, dann macht die etwas völlig anderes. Die macht SAX und parsed das Dokument nur so weit wie nötig und wenn sie den ersten Body gefunden hat, ist das Parsing zu Ende. Bei dieser Verarbeitung wird der erste fett gedruckte Datensatz verwendet. Sie haben also hier zwei völlig verschiedene Sichten auf diese Daten. Das hätte man natürlich ausnutzen können, um eigene Programme unter einer Fremden ID in der Cloud ausführen zu lassen.

Fehlerhafte Signaturverifikation in der Amazon Cloud

Wie die Signaturverifikation (DOM) die (XML-)Welt sieht



Wie die Geschäftslogik (SAX) die (XML-)Welt sieht

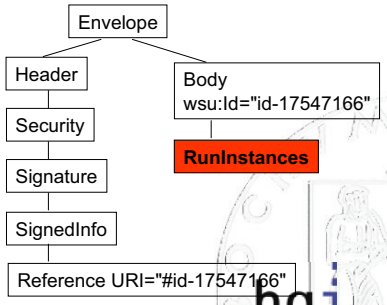


Bild 21

Fehlerhafte Signaturverifikation in der Amazon Cloud

- Signaturverifikation verwendet DOM:
  - Zuerst wird der erste Body in den Hauptspeicher geladen
  - Dann wird der zweite Body in den Hauptspeicher geladen: da er ein identisches ID-Attribut besitzt, wird der erste Body mit dem zweiten überschrieben
  - Somit sind die tatsächlich signierten Daten geladen, und die Signaturverifikation ist erfolgreich
- Businnes Logic verwendet SAX:
  - BL wartet auf den Event, dass der Body der SOAP-Nachricht geladen wird.
  - Sobald dieser Event eintritt, werden die Daten verarbeitet, in diesem Fall die nicht signierten Daten.
  - Tritt der gleiche Event zum zweiten Mal auf (der Original-Body wird geladen), wird er ignoriert.

Bild 22

Bei Amazon ist das behoben (Bild 21, 22). Woanders kann der Fehler natürlich auch auftreten. Aber er ist genau wie der andere Angriff publiziert und Gegenmaßnahmen dazu auch. Es muss nur umgesetzt werden. Wir haben das in Gesprächen mit der Industrie schon oft thematisiert. Da wird dann oft gesagt: Ja, aber meine Policy sagt doch…. Die Policy ist nicht relevant, sondern dass, was nachher über die Leitung geht, was geschickt wird. Da fehlt noch ein bisschen das Verständnis.

Bild 23

Wo kommen die beiden Welten (Browser und Webservices) zusammen? Jetzt komme ich wieder Thema Identitätsmanagement zurück (Bild 23). Die beiden Welten kommen zum Beispiel beim Single Sign-On zusammen. Da ist es so, dass vom Urahn der Single Sign-On Protokolle Microsoft Passport schon vor Jahren generische Schwachstellen publiziert wurden. Man benutzt einen Browser und bekommt irgendwann ein Ticket zurück, mit dem man sich bei der Relying Party einloggen kann. Das ist aber nur locker im Browser gespeichert, d.h. man kann es stehlen. Man kann es entweder über Angriffe wie Cross Site Scripting stehlen – das war damals einer der publizierter Angriffe auf MS Passport – oder man könnte es zum Beispiel durch einen Man in the Middle Angriff auf diese Verbindung zur Relying Party stehlen.

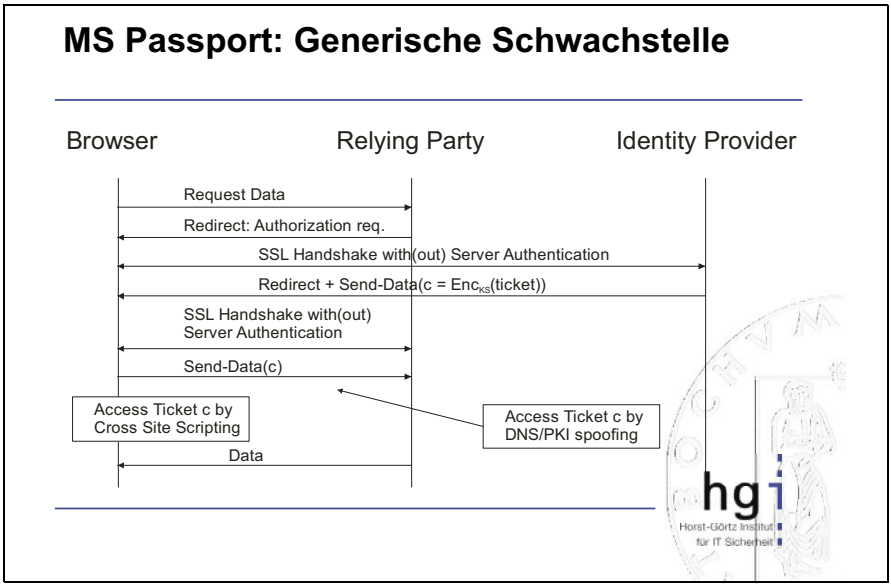


Bild 24

Diese Schwachstellen stecken in fast allen heutigen Single Sign-On Protokollen auch noch drin (Bild 24).

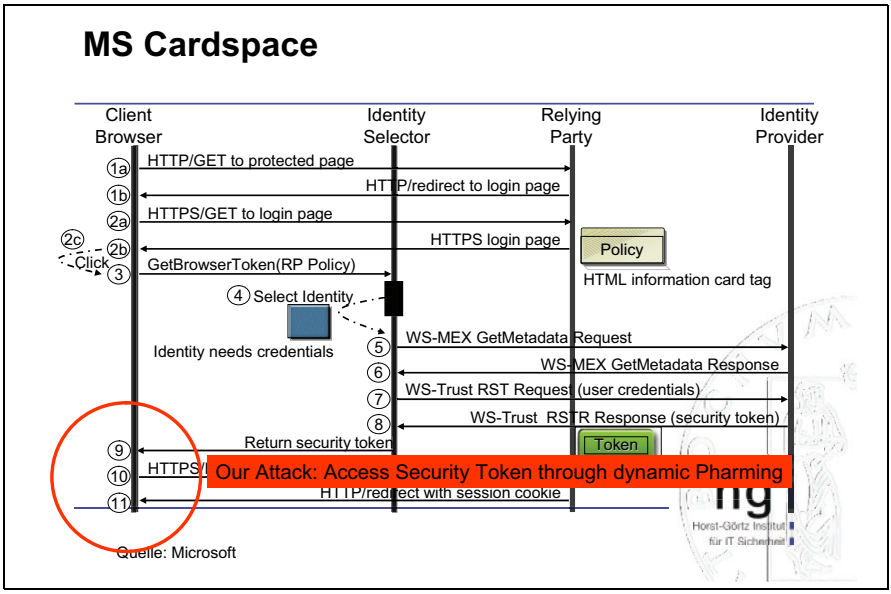


Bild 25

Eine rühmliche Ausnahme möchte ich erwähnen und zwar ist das Herr Klingenstein aus der SAM L-Standardisierungsgruppe, der sich Gedanken darüber gemacht hat, parallel zu uns übrigens, wie man hier SSL Client Zertifikate einsetzen kann (Bild 25). Dabei ist eine wasserdichte Lösung herausgekommen. Bei dieser Lösung können Sie die Tokens zwar noch aus dem Browser stehlen, sie können sie aber nicht von einem fremden Browser aus einlesen. Diese Lösung kann man mit Chipkarten soweit ausbauen, dass da keine Angriffe mehr möglich sind. Es gibt Ansätze, und das funktioniert auch ohne PKI. All die Probleme, die sie vielleicht noch im Hinterkopf haben, Client Zertifikat, PKI, Rollout – vergessen Sie es. Sie brauchen keinen PKI dafür. Das können selbst signierte Zertifikate sein.

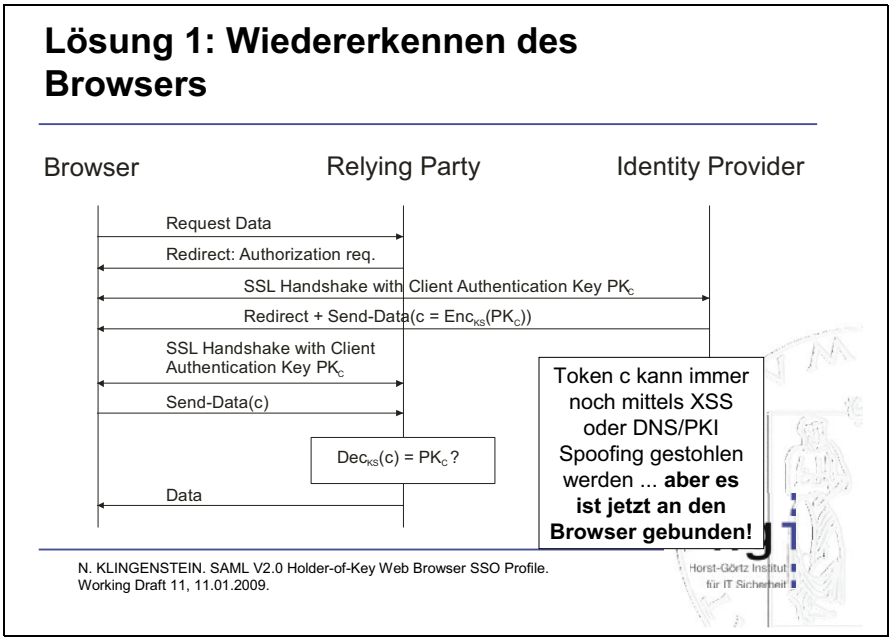


Bild 26

Da kommt zusammen: SAML ist XML basiert, hat eine XML Signatur (Bild 26). In diese Signatur werden Informationen aus dem Browser mit aufgenommen, so dass das Ganze ein wasserdichtes System wird, ein sehr komplexes System, zwei Server, ein Browser, ganz viele Protokolle. Aber man kann das Problem lösen. Man kann es noch anders lösen, was aber dann technisch komplexer wird. Daran arbeiten wir auch, indem wir den Browser etwas stärker machen (Bild 27).

Lösung 2: Wiedererkennen des Servers

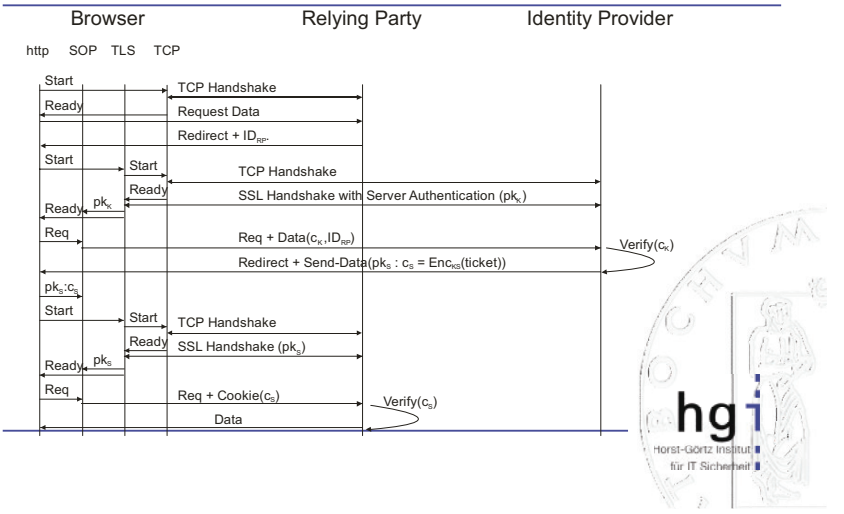


Bild 27

Überblick

1. Die wirklichen Bedrohungen im Cloud Computing
2. Der Webbrowser als universelle Client-Software in der Cloud
3. Webservices: Die Sprache der Cloud
4. Single Sign On
5. Ausblick: Was noch zu tun ist

Bild 28

Ich möchte zum Ausblick kommen (Bild 28). Was ist noch zu tun? Wenn wir den Browser als Client Software nutzen wollen, sind noch kleine Änderungen zu machen. Die lassen sich natürlich nicht im deutschen Alleingang durchsetzen. Das muss international diskutiert werden, auch mit den Herstellern. Insbesondere finde ich es wichtig, dass diese beiden Sicherheitspolicies im Browser endlich miteinander reden. Auch dazu gibt es schon Publikationen. So können über den Public Key des Server Zertifikate nebeneinander gekoppelt werden. Eine andere Lösung sind Client Zertifikate, die bislang sehr selten eingesetzt werden, die aber eine große Bedeutung bekommen werden, weil sie eben schon heute eingesetzt werden können. Jeder Browser unterstützt das. Die Lösungen sind erst einmal wasserdicht und man braucht keine PKI dafür. Die alten Probleme tauchen eigentlich nicht auf.

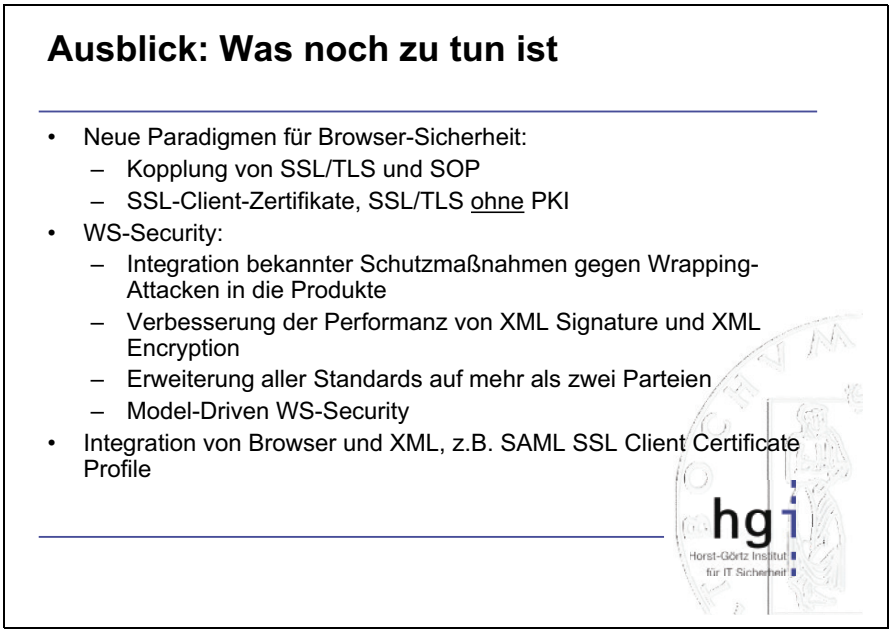


Bild 29

Im Bereich XML müssten [Gegenmaßnahmen gegen] diese Wrapping Angriffe in die Praxis hineingetragen werden (Bild 29). Es gibt Lösungen, die sind publiziert und auch nicht sehr teuer umzusetzen. Hier fehlt noch ein bisschen das Verständnis, auch weil es vielleicht noch nicht viele dokumentierte Angriffe hierauf gibt. Die Performanz von XML-basierten kryptografischen Mechanismen muss verbessert werden. Daran arbeiten die Standardisierungsgremien. Man hat gemerkt, dass man etwas zu komplexe Standards gebaut hat. Die Standards haben immer noch dieses Client Server Paradigma im Hinterkopf. Wenn Sie sich die Standards genauer

anschauen, funktionieren die meist sehr gut bei zwei Parteien. Aber heute orchestriert man ganze Prozessketten und da muss man etwas tun, um das auf diese Prozessketten zu übertragen. Ein möglicher Ansatz dafür wäre so etwas wie Model-Driven WS-Security, ein grafisches Modellierungstool, wo Sie Ihre Prozesse modellieren und dann auch Sicherheitsannotationen daran setzen können, die dann automatisch in eine gute Implementierung umgesetzt werden. Die Integration von Browser und XML wie es schon am Beispiel der SSL Client Zertifikate und SAML Tokens hier vorgenommen wurde, muss man vorantreiben. Ich denke, das sind die beiden wichtigen Tools, die man in Zukunft benutzen wird.

Veröffentlichungen zum Thema (Bild 30).

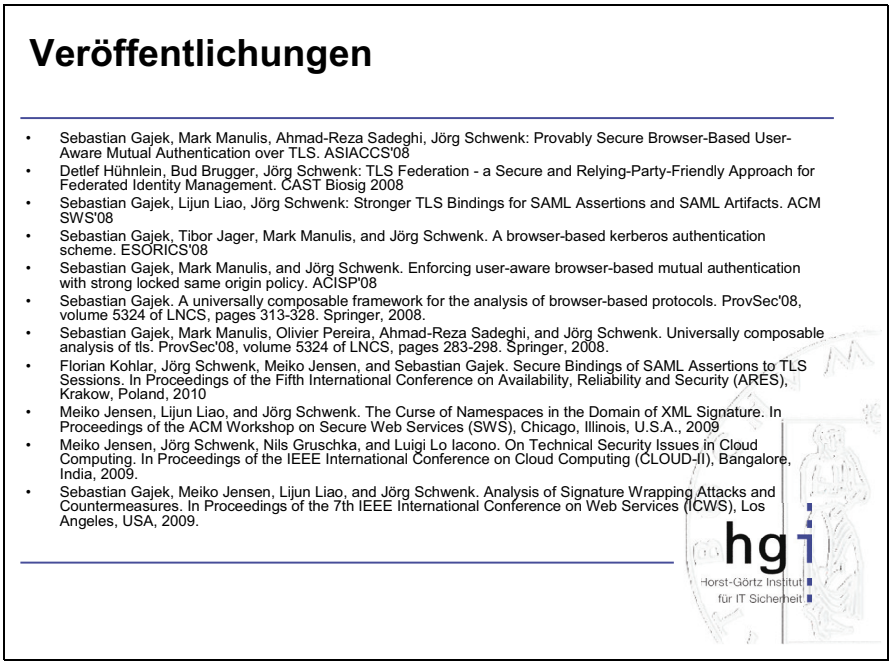


Bild 30

7 Maßnahmen der Politik zur Bildung und Erhaltung von Vertrauen in die Sicherheit und Zuverlässigkeit der ITK-Versorgung

Martin Schallbruch
Bundesministerium des Innern, Berlin

In dieser Veranstaltung, in der es um Cloud Computing geht und in vielen Vorträgen, z. B. dem Vortrag von Herrn Prof. Schwenk, um die Sicherheit von Cloud Computing, möchte ich den Bogen etwas weiterspannen und die Frage der Sicherheit der Informationstechnik und des Internet insgesamt in den Fokus meiner Ausführungen rücken. Vor dem Hintergrund des Koalitionsvertrags der neu gebildeten Bundesregierung, die heute 100 Tage im Amt ist wie Sie den Zeitungen entnehmen können, möchte ich darstellen, was aus Sicht der Bundesregierung die wesentlichen Maßnahmen sind, die bei der IT-Sicherheit jetzt angegangen werden.

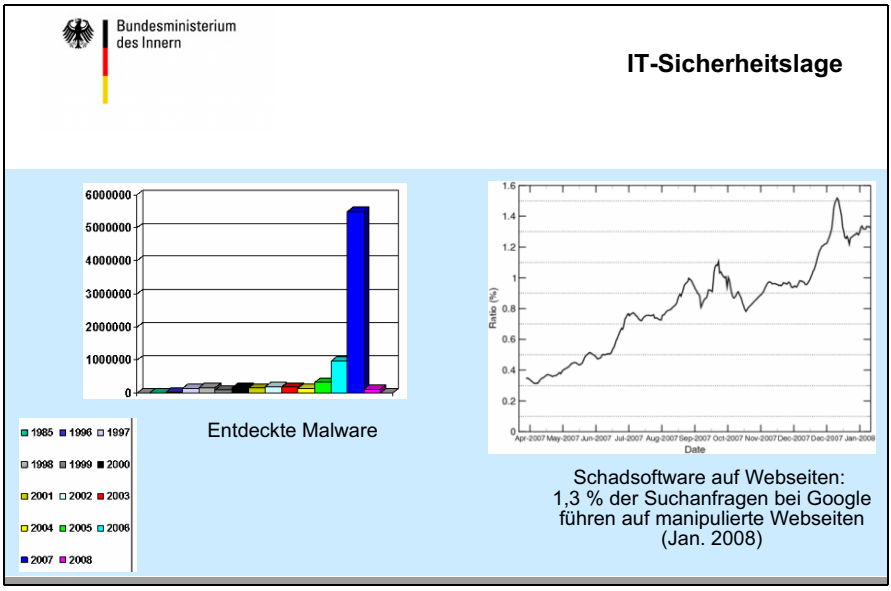


Bild 1

Einleitend ein paar Worte zur IT-Sicherheitslage (Bild 1). Ich will nicht viel dazu ausführen, weil ich viele Experten hier im Raum sehe und ich Ihnen im Übrigen den Bericht des Bundesamtes für Sicherheit in der Informationstechnik zur Lage der

A. Picot et al. (eds.), *Trust in IT*, DOI 10.1007/978-3-642-18110-8_7,

IT-Sicherheit für das Jahr 2009 empfehlen würde, wenn Sie hier weiteren Informationsbedarf haben. Zwei Dinge, die mir persönlich besonders bedeutend erscheinen, will ich herausheben:

Zum Einen, dass Schadprogramme sowohl in der Quantität als auch in der Qualität ständig zunehmen. Das heißt, wir haben eine immer neue Art von Programmen, neue Plattformen, immer neue Mechanismen usw. Und wir haben aber auch gleichzeitig eine quantitative Steigerung der entdeckten Schadprogramme, wie Sie der gezeigten Kurve aus den Jahren bis einschließlich 2007 und den gewaltigen Steigerungsraten entnehmen können.

Das Zweite, was ich sehr besorgniserregend finde, ist, dass der Verbreitungsweg für Schadprogramme im Internet zunehmend das Ansurfen von Webseiten ist, die Schadgut enthalten. Das sind häufig genug Websites, die manipuliert worden sind, herkömmliche, gut beleumundete, etablierte Websites, die Sicherheitslücken haben, manipuliert worden sind und dann zum Träger und Verbreiter von Schadgut werden. Das Bild zeigt, wie viel Prozent der Suchangabenergebnisse, wenn man eine Googlesuche macht, auf manipulierte Websites führt – heute schon eine größere Anzahl von Websites. Das BSI empfiehlt daher den Behörden, dass man auf aktive Inhalte in den Websites weitgehend verzichten soll. Aber wer verzichtet heute schon auf aktive Inhalte und welche Anwendungen kann man überhaupt noch nutzen, wenn man auf aktive Inhalte verzichtet?

Wozu führt diese veränderte Sicherheitslage? Sie führt zu einer Vielfalt von Angriffsmöglichkeiten und Angriffen auf die IT- und Datensicherheit, Angriffe auf die Integrität und Benutzbarkeit von IT-Systemen. Wir haben eine Vielzahl von Denial of Service Attacks, sowohl gegen Unternehmen als auch gegen Behörden, gesteuert von Botnetzen, in denen sich ahnungslose Bürger mit ihren Rechnern verfangen haben. Das führt zum Angriff auf die Vertraulichkeit. Wir haben solche Angriffe bei den Rechnern der Bundesregierung von Seiten ausländischer Stellen, die versuchen, auf die Art an Geheimnisse zu kommen, klassische Spionageangriffe. Es gibt einen sich vermehrenden Identitätsbetrug und Identitätsdiebstahl.

Das Ganze ist heutzutage arbeitsteilig von der organisierten Kriminalität gesteuert. Da gibt es Gruppen, die solche Trojaner entwickeln und für ihre Verbreitung sorgen. Da gibt es Gruppen, die Botnetze betreiben und vermieten. Da gibt es andere Gruppen, die sogenannte Drop-Zones betreiben und dort Identitätsdaten, die gestohlen worden sind und dort abgelegt sind, sortieren, um dann tausende E-Mail-Accounts oder Kreditkartendaten verkaufen zu können. Solchen Ketten sind aus Sicht der Sicherheitsbehörden relativ schwer zu ermitteln, weil die Geschäftsanbahnung und die Organisation nur online läuft.

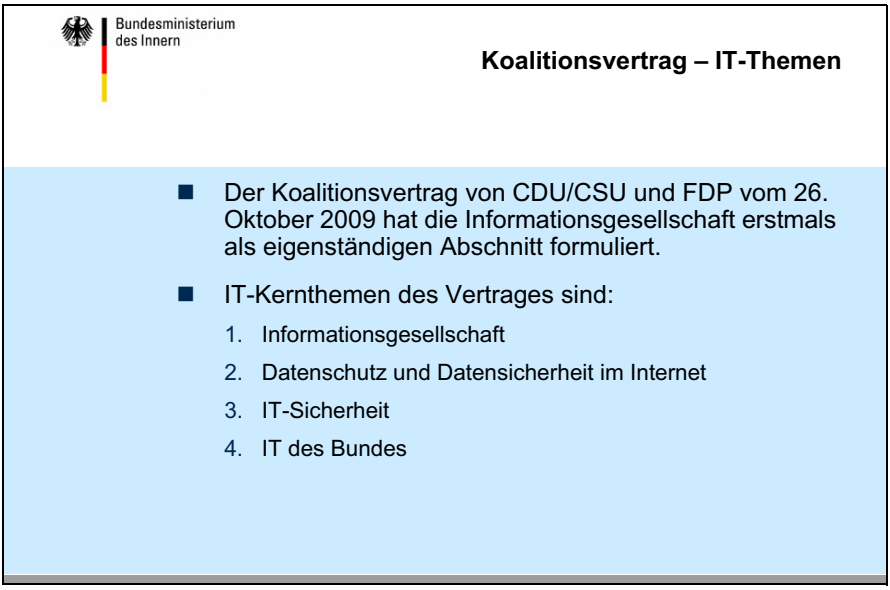


Bild 2

Vor dem Hintergrund dieser Lage, gab es in den Koalitionsverhandlungen zwischen CDU/CSU und FDP im letzten Oktober eine ernsthafte Diskussion über die Frage, wie wir mit dem Thema Informationsgesellschaft und Sicherheit der Informationsgesellschaft umgehen (Bild 2). Sie haben vielleicht gesehen, dass der Koalitionsvertrag der die Bundesregierung tragenden Koalition dem Thema Informationsgesellschaft erstmals einen eigenen Abschnitt widmet und dort beschreibt, welche Ziele mit welchen Maßnahmen verfolgt werden sollen. Datenschutz und Datensicherheit im Internet und die IT-Sicherheit der Einrichtungen des Bundes und der kritischen Infrastrukturen sind dort sehr prominent vertreten.

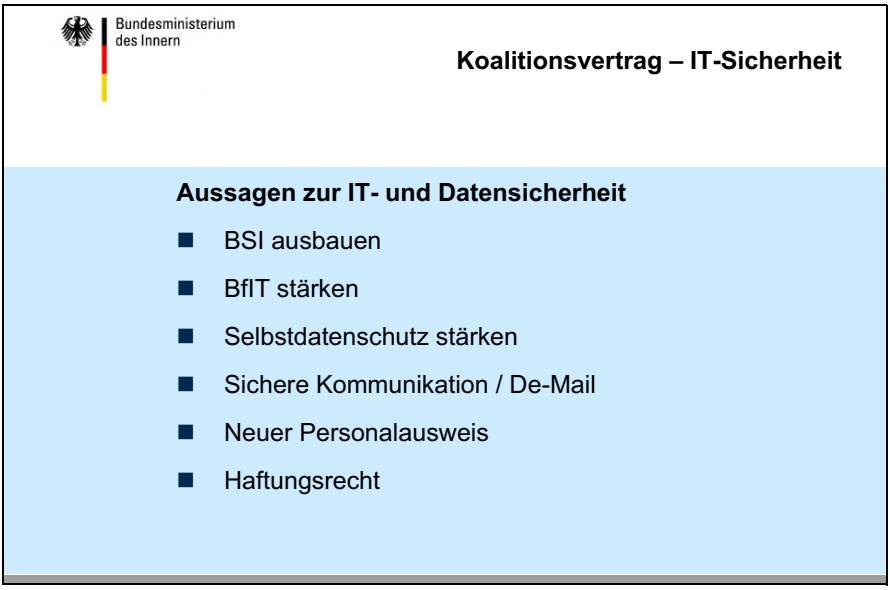


Bild 3

Im Einzelnen gibt es zur IT- und Datensicherheit eine ganze Reihe von Verpflichtungen, die sich aus dem Koalitionsvertrag ableiten und die die Bundesregierung jetzt umzusetzen hat (Bild 3). An mehreren Stellen ist erwähnt, dass das BSI als Zentrale IT-Sicherheitsbehörde in Deutschland ausgebaut werden soll und zwar zum einen, um die Infrastruktur des Staates zu schützen, d.h. unser Land auch gegen Cyberangriffe zu schützen, zum anderen aber auch, um Hilfestellung zu leisten, dass die Menschen sich selbst schützen können, dass Selbstschutz und Eigenschutz verbessert wird. Dafür sind Technologien bereitzustellen, Aufklärung zu betreiben usw. Mit beiden Zielrichtungen werden wir in den nächsten Jahren das BSI stärken und befinden uns jetzt, wie Sie sich denken können, in schwierigen Haushaltsverhandlungen, um das umzusetzen.

Eine zweite Aussage des Koalitionsvertrags ist, dass die Funktion der Beauftragten der Bundesregierung für Informationstechnik – seit heute ist es Frau Staatssekretärin Rogall-Grothe – gestärkt werden soll, um ihr mehr Möglichkeiten zu geben, die Sicherheit der IT-Systeme der Bundesbehörden zu gewährleisten und damit auch die Funktionsfähigkeit der staatlichen Instanzen für den Fall eines IT-Angriffs. Es gibt in der Koalitionsvereinbarung eine Reihe von Verpflichtungen, die helfen sollen, den Selbstdatenschutz zu stärken, die Menschen in die Lage zu versetzen, sich selbst zu helfen. Dazu komme ich gleich mit einem Beispiel. Erwähnt sind im Vertrag auch Projekte, die wir schon in der letzten Wahlperiode aufgesetzt haben und in dieser Wahlperiode zum Abschluss bringen, wie die Sicherheit im Internet, sichere Kommunikation mit De-Mail oder der neue Perso-

nalausweis. Es gibt auch die Verpflichtung, dass wir uns damit auseinandersetzen, ob wir zur Verbesserung der Sicherheit im Internet nicht Änderungen im Haftungsrecht vornehmen müssen, um die Risikoverteilung zwischen den Akteuren, den Providern, den Anbietern, den Kunden, denjenigen, die Komponenten dazu bereitstellen, um diese Risikoverteilung vernünftig abzubilden und nicht alles beim Endkunden abzuladen. Da sind wir aber mit unseren Überlegungen noch ganz am Anfang.

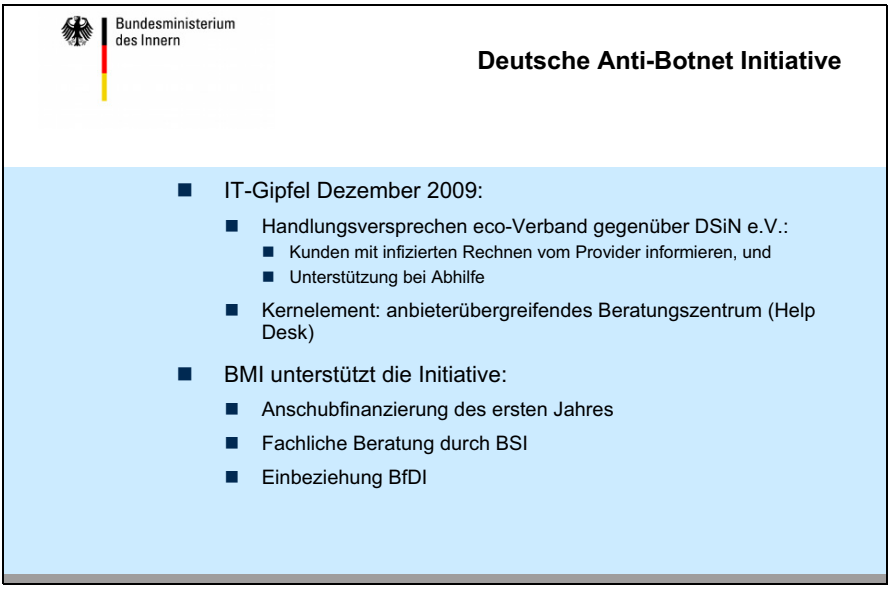


Bild 4

Ich will einige der Maßnahmen etwas prominenter hervorheben, um Ihnen einen Einblick in den Sachstand zu geben (Bild 4).

Dem Schutz der Bürgerinnen und Bürger dient eine Initiative, die wir zum letzten IT-Gipfel im Dezember 2009 gestartet haben gemeinsam mit eco. Eco – der Verband der Internetwirtschaft – hat diese Idee entwickelt, die Menschen darin zu unterstützen, ihre Rechner aus Botnetzen herauszuholen. Sie müssen zunächst einmal merken, dass ihr Rechner Teil eines Botnetzes ist und dann eine Hilfestellung haben, wie sie ihn wieder herausbekommen. Der ecoVerband und die dort organisierten Provider haben sich im Rahmen dieser Initiative dazu verpflichtet, die Kunden, die entsprechend infizierte Rechner haben, darüber zu informieren, wenn ein Rechner in einem Botnetz ist. Das merkt man z.B. an Verbindungen zu sog. Command-and-Control-Servern, die aufgenommen werden. Dem Kunden soll vom Provider gleichzeitig ein Angebot gemacht werden für eine Information, wie man solche Trojaner entfernt. Darüber werden die Provider eine Hotline aufbauen, die

die Kunden dann anrufen können, wenn sie Beratung brauchen, wie sie weiter vorgehen können. Man wird das nicht alles am Telefon klären können. Das ist klar. Es hängt auch immer vom Wissen des Kunden ab. Aber der Kunde hat durch diese Initiative künftig den Vorteil, dass er die Information bekommt, dass der Rechner im Botnetz ist, zum Beispiel an einer Denial of Service Attack mitwirkt, weil ein Trojaner auf dem Rechner ist. Und mit der Hotline hat der Kunde jemanden, den sie oder er anrufen kann, fragen kann, was zu tun ist, an wen man sich wenden kann und wo es Informationen gibt. Die Bundesregierung unterstützt diese Initiative durch eine Anschubfinanzierung im ersten Jahr sowie durch eine fachliche Beratung durch das BSI. Außerdem haben wir eine Einbeziehung des Bundesbeauftragten für den Datenschutz vorgesehen, um von Anfang an klarzumachen, dass die Initiative datenschutz-konform realisiert wird, dass hier keine Daten von den Providern an irgendwen übermittelt werden, sondern dass es nur darum geht, dass der Provider, wenn er solche Indikationen für Botnetze hat, den Kunden informiert. Diese Daten werden auch nicht gesammelt oder sonst wie verarbeitet. Das hat der BfDI sich angesehen und für vernünftig gehalten.

Bild 5

Zweites Beispiel ist der neue Personalausweis (Bild 5). Wir haben im letzten Jahr das neue Personalausweisgesetz im Bundestag verabschiedet. Es tritt zum 1.11.2010 in Kraft. Wir werden ab 1.11.2010 einen neuen Personalausweis an alle Bürgerinnen und Bürger ausgeben, die ab dem 1.11. einen neuen Ausweis beantragen. Der, dessen Ausweis noch nicht abläuft, kann trotzdem einen neuen Ausweis beantragen. Das ist eine Ausnahme, damit jeder, der will, frühzeitig in den Genuss der elektro-

nischen Funktion dieses Ausweises kommt. Diese elektronische Funktion des Ausweises – das Gesetz nennt das elektronischer Identitätsnachweis – ist diejenige, die den neuen Ausweis zu einem Beitrag für mehr Sicherheit im Internet macht. In dem Personalausweis ist ein kontaktloser Chip enthalten, der es ermöglicht, dass man sich im Internet gegenüber einem Diensteanbieter identifiziert, der eine entsprechende elektronische Identifizierung im Internet haben will oder auch offline gegenüber Automaten identifiziert.

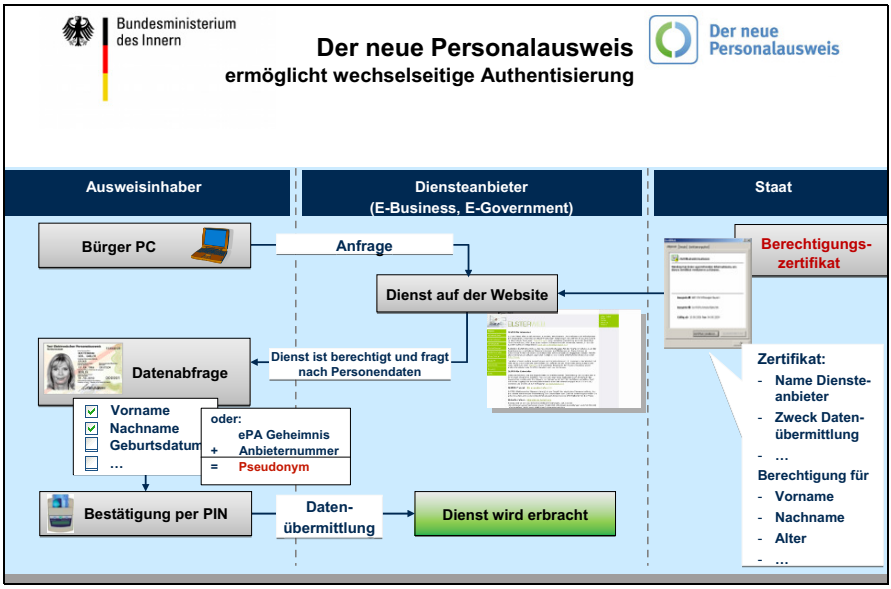


Bild 6

Das Besondere an der Architektur des neuen Ausweises ist, dass bei der Ausgestaltung der Datenschutz ganz oben steht (Bild 6). Wenn Sie sich einmal anschauen, auch beispielsweise mit dem vergleichen, was es in anderen Staaten, Estland, Niederlande, Spanien, Portugal schon gibt, werden Sie sehen, dass im deutschen Konzept der Datenschutz im Mittelpunkt steht. Der Personalausweis gibt seine Daten nur dann frei, wenn der Diensteanbieter vorher beim Bundesverwaltungsamt eine Berechtigung erworben hat, die elektronische Identitätsfunktion zu nutzen. Dazu muss der Diensteanbieter angeben, zu welchen Zwecken er die Daten braucht, welche Datenschutzaufsichtsbehörde zuständig ist und welche Daten aus dem Personalausweis verwendet werden können. Jeder Anbieter im Internet kann entscheiden, eine Identifizierung mit dem Ausweis vorzusehen, etwa um anschließend eine Bestellung per Rechnung statt Vorkasse zu ermöglichen. Gegenüber dem Kunden wird das über die Website kommuniziert und wenn der Kunde diese Möglichkeit nutzen will, dann legt er im ersten Schritt seinen Personalausweis auf das Lesegerät. Der Diensteanbieter muss anschließend ein Berechtigungszertifikat an

den Ausweis übermitteln. Dieses Berechtigungszertifikat wird vom Ausweis geprüft und die Software zeigt dem Nutzer an, dass der Diensteanbieter eine Berechtigung zum Zugriff auf die Daten hat, wann und wie lange die Berechtigung gilt, wer die zuständige Datenschutzaufsichtsbehörde ist und welche Daten aus dem Ausweis genutzt werden sollen. Das können Name und Anschrift sein oder nur das Alter für die Altersverifikation – ohne das konkrete Geburtsdatum zu übermitteln – oder auch ein Pseudonym. Im dritten Schritt kann der Kunde dann durch Eingabe seiner PIN im Einzelfall die Datenübermittlung bestätigen. Wenn einer der Anbieter diesen Mechanismus missbraucht, wird ihm die Berechtigung entzogen. Das Bundesverwaltungsamt kann jederzeit diese Berechtigung entziehen und auch technisch wirksam binnen 24 Stunden sperren.

Wir werben für dieses Konzept, weil damit ein Standardidentitätsinstrument für die digitale Welt bereitgestellt wird. Hiervon profitieren Diensteanbieter, indem sie eine staatlich verbürgte Identifizierung im Netz erhalten, die auf Chipkartensicherheit beruht. Hiervon profitieren Kunden, die Licht im Dschungel der unterschiedlichen Identifizierungsinstrumente im Internet haben.

Natürlich ist der Aufwand für die Identifizierung mit dem Personalausweis – ich habe den Ablauf beschrieben – keine Identifizierung im Vorübergehen. Manche Anwendungsanbieter haben daher entscheiden, dass das etwas für die Erstregistrierung oder für besonders hochwertige Transaktionen ist. Wir teilen diese Einschätzung und gehen nicht davon aus, dass der elektronische Identitätsnachweis des neuen Ausweis zukünftig jede Transaktion absichert. Das ist völlig in Ordnung. Dieses hochwertige Authentisierungsinstrument steht zukünftig zur Verfügung und damit eine Möglichkeit, aus dem bisherigen Wildwuchs herauszukommen.

Man kann auf Wunsch übrigens auch eine qualifizierte elektronische Signatur auf den Personalausweis laden. Die Karte ist für die Signatur vorbereitet.

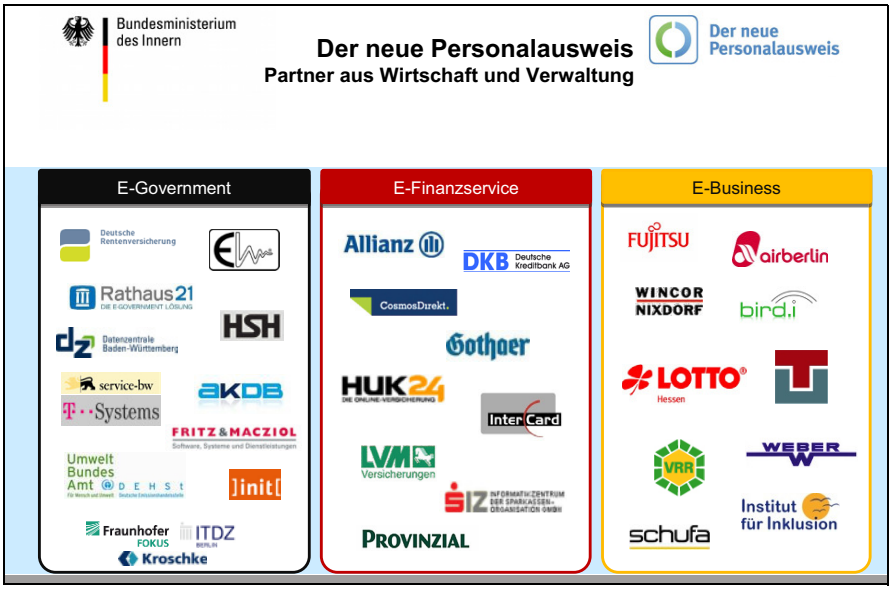


Bild 7

Im Augenblick bereiten sich die Meldestellen in Deutschland auf die Ausgabe ab 1.11. vor. Wir haben parallel dazu einen Anwendungstest begonnen, in dem sich Partner aus Wirtschaft und Verwaltung auf die Nutzung dieser Karte in ihren elektronischen Anwendungen vorbereiten (Bild 7). Es gibt einige Partner, mit denen wir sehr eng zusammenarbeiten, die also mit unserer Unterstützung diese Vorbereitung durchführen, sich ertüchtigen und auch erproben, wie man den Personalausweis in Geschäftsprozesse integrieren kann. Die Logos dieser Partner sehen Sie hier auf der Folie. Einige sitzen, wie ich festgestellt habe, auch hier im Raum.

Dahinter stehen jeweils ganz unterschiedliche Anwendungsszenarien. Ob das der Check in bei der Fluggesellschaft ist, die Abwicklung von Versicherungsverträgen bei einer Versicherung, eGovernment-Dienstleistungen bei einer Stadtverwaltung, der Zugriff auf das Rentenversicherungskonto oder die Auskunft über die SCHUFA-Daten. Das sind ganz unterschiedliche Anwendungen, die alle auf diese Form der Identifizierung setzen und die sich im Augenblick darauf vorbereiten.

Neben diesen 30 Partnern, die wir sorgfältig ausgewählt haben, um die ganze Breite der Anwendungsmöglichkeiten systematisch abzudecken, gibt es für jedes Unternehmen die Möglichkeit, sich in dem sogenannten offenen Anwendungstest zu beteiligen. Die Teilnehmer bekommen alle Informationen und auch die Module und die Software, aber sie bekommen keine exklusive Betreuung durch das für den Anwendungstest eingerichtete Kompetenzzentrum. Für diese zusätzliche Möglich-

keit haben sich etwa 100 Unternehmen deutschlandweit entschieden und sind dabei, in diesen Test mit einzusteigen.

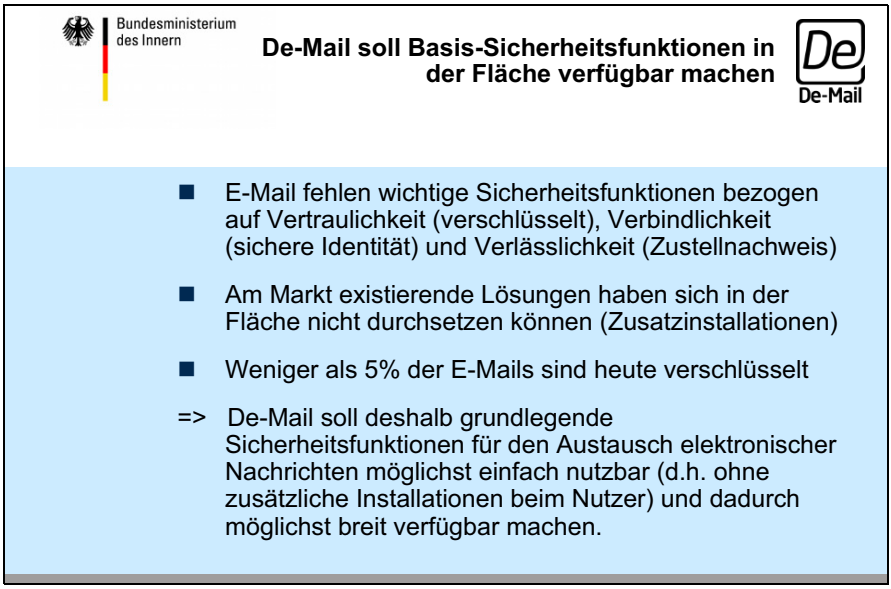


Bild 8

Ein weiteres Projekt, das im Koalitionsvertrag angelegt ist und das wir nun zu Ende bringen werden, ist De-Mail (Bild 8). De-Mail soll mehr Sicherheit ins Internet bringen, indem der herkömmliche E-Mail-Dienst um eine Lösung für sichere und verlässliche elektronische Nachrichten ergänzt wird. De-Mail soll die Probleme, die wir heute mit der Zustellung von E-Mails haben – man weiß nicht, welcher Absender das ist, die E-Mail ist nicht verschlüsselt, man kann nie sicher sein, ob eine E-Mail, die man versendet, auch ankommt – lösen und vor allen Dingen helfen, dass wir zu flächendeckenden Lösungen kommen, die auch interoperabel sind. Das ist ja bislang nicht der Fall. Es gibt alle möglichen Angebote auf diesem Feld. Es gibt Individualsoftware. Es gibt Angebote einzelner Provider.

Bild 9

Der Ansatz bei De-Mail ist, die Anforderungen an Sicherheit, Funktionalität und Interoperabilität durch Richtlinien des BSI festlegen zu lassen, auf deren Basis die Provider De-Mail konforme Dienste anbieten und sich zertifizieren lassen zu können (Bild 9). Voraussetzungen für die Zertifizierung sind Datenschutz, Interoperabilität, Sicherheit. Der Provider muss auch sicherstellen, dass mit jedem anderen De-Mail-zertifizierten Provider kommuniziert werden kann. Er muss auch sicherstellen, dass ein De-Mail-Konto übertragen wird, wenn man wechseln will.

De-Mail wird E-Mail nicht ersetzen, sondern es eine zusätzliche Versendungsmöglichkeit mit bestimmten Sicherheitseigenschaften bieten und den Menschen helfen, weiterhin mit ihren Standardprovidern zu arbeiten, zukünftig aber auch sicher E-Mails versenden zu können.

Aus Sicht der Unternehmen ist es interessant, dass man Vorgänge, die bislang noch per Papier versendet werden, Versicherungsunterlagen beispielsweise, zukünftig mit De-Mail versenden kann, weil man Absenderauthentisierung hat, weil man Verschlüsselung hat und weil man weiß, dass man eine Zugangsbestätigung bekommt, wenn etwas zugestellt worden ist. Dieses Projekt ist kein Projekt, in dem der Staat eine IT-Infrastruktur aufbaut, sondern lediglich ein Zertifizierungsverfahren und eine gesetzliche Verankerung, dass nur die sich De-Mail-Provider nennen dürfen, die das Zertifizierungsverfahren durchlaufen haben.

Wir sind im Augenblick in einem Pilotversuch in der Stadt Friedrichshafen, zusammen mit vielen Partnern aus Wirtschaft und Verwaltung, der bis Ende März läuft. Ich gehe davon aus, dass wir im Anschluss an das Pilotverfahren die Diskussion im Bundestag über das nötige De-Mail Gesetz wiederaufnehmen werden.

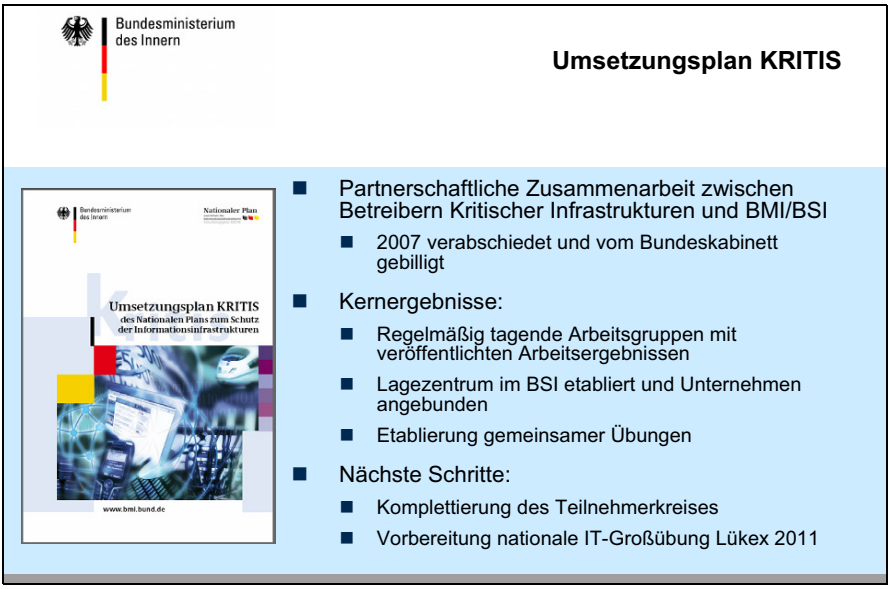


Bild 10

Diese vorgestellten Dinge, die Anti-Botnetz-Initiative, Personalausweise, De-Mail sind Beiträge, die darauf zielen, den Bürgerinnen und Bürgern Möglichkeiten an die Hand zu geben, mit der komplexen Sicherheitslage im Internet einfacher umzugehen (Bild 10).

Zwei andere Zielrichtungen unserer IT Sicherheitspolitik möchte ich noch erwähnen, nämlich die Zusammenarbeit mit den Trägern kritischer Infrastrukturen zum Schutz der IT der kritischen Infrastrukturen. Manche von Ihnen wissen, dass wir 2007 mit den Betreibern kritischer Infrastrukturen, z.B. Finanz- und Verkehrsunternehmen, Energieversorger und anderen, einen sogenannten Umsetzungsplan KRITIS vereinbart haben, der die Informationssicherheit in den kritischen Infrastrukturen adressiert und auch Strukturen der Zusammenarbeit zwischen den Infrastrukturträgern und zwischen ihnen und dem Staat etabliert. Diese Strukturen sind zum Teil schon funktionsfähig, zum Teil noch im Aufbau. Es gibt Branchen, die schon besonders operativ sind – die Versicherungsbranche beispielsweise, die sich sehr schnell bewegt hat und auch ein entsprechendes Lagezentrum angestoßen hat. Wir sind jetzt dabei, aus diesen Strukturen am Ende eine funktionierende deutschlandweite IT Kriseninfrastruktur zu machen, die auch in der Lage ist, in einer

schwierigen Situation belastbar zusammenzuarbeiten. Wir haben uns vorgenommen, der Bund, die Länder, gemeinsam mit den Partnern aus den kritischen Infrastrukturen im Rahmen einer länderübergreifende Krisenübung das im Herbst 2011 zu üben. Da werden wir zwei Tage mit Krisenstäben auf allen Ebenen die Reaktion auf einen IT-Angriff üben, um zu schauen, wie die Mechanismen der Zusammenarbeit zwischen den kritischen Infrastrukturbetreibern und dem Staat funktionieren. Das ist deshalb so wichtig, weil ein Großteil der kritischen Infrastrukturen privat betrieben wird und weil im Falle eines IT Angriffs oder eines großflächigen Ausfalls eine enge Zusammenarbeit mit den Sicherheitsbehörden und mit den Katastrophenschutzbehörden erfolgen muss.

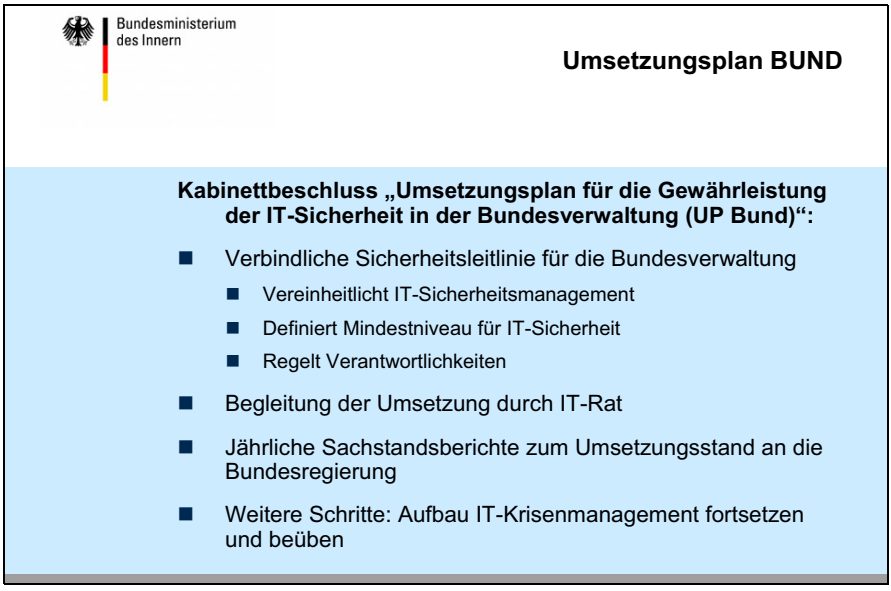


Bild 11

Daneben kümmern wir uns natürlich auch um unsere eigenen IT-Infrastrukturen. Eine der ganz wichtigen Aufgaben des BSI und des Innenministeriums ist, dafür zu sorgen, dass wir ein funktionierendes IT Sicherheitsmanagement für die Behörden des Bundes haben (Bild 11). Dazu gibt es einen Beschluss des Bundeskabinetts, der ein IT-Sicherheitsmanagement etabliert. Das ist mittlerweile aufgesetzt. Wir haben in allen Behörden IT-Sicherheitsbeauftragte. Wir haben IT-Sicherheitsbeauftragte der Ministerien, die für den Geschäftsbereich ihrer Ministerien koordinieren, dass ihre Behörden gut aufgestellt sind. Wir haben ein ziemlich hartes Berichtswesen. Es gibt immer regelmäßige Ampelstatusberichte, die klar machen, welche Verpflichtungen umgesetzt worden sind. Viele Behörden haben eine ganze Vielzahl von Verpflichtungen, die umgesetzt werden müssen. Die permanente Gewährleistung der IT-Sicherheit ist nicht ganz einfach, weil die Behörden aufgrund der Anforderungen

der Politik immer neue IT-Projekte aufzusetzen haben, auch weil die Unternehmen mehr eGovernment wollen und weil auch die Bürgerinnen und Bürger mit dem Staat elektronisch zusammenarbeiten wollen. E-Government ist auch ein Teil meines Verantwortungsbereichs. Für eine Behörde ist es immer ausgesprochen schwierig, angesichts dieser starken Erwartungen von außen gleichzeitig so priorisieren, dass hinreichend viele Ressourcen für IT-Sicherheitsmanagement vorhanden sind. In den Unternehmen ist das nicht viel anders und insofern ist das ein Thema, was uns miteinander verbindet, dass wir dem IT-Sicherheitsmanagement, gerade der Organisation und der Stärkung der Verantwortlichen und der sachgerechten Ausstattung der IT-Sicherheitsbeauftragten, hinreichend viel Aufmerksamkeit widmen.

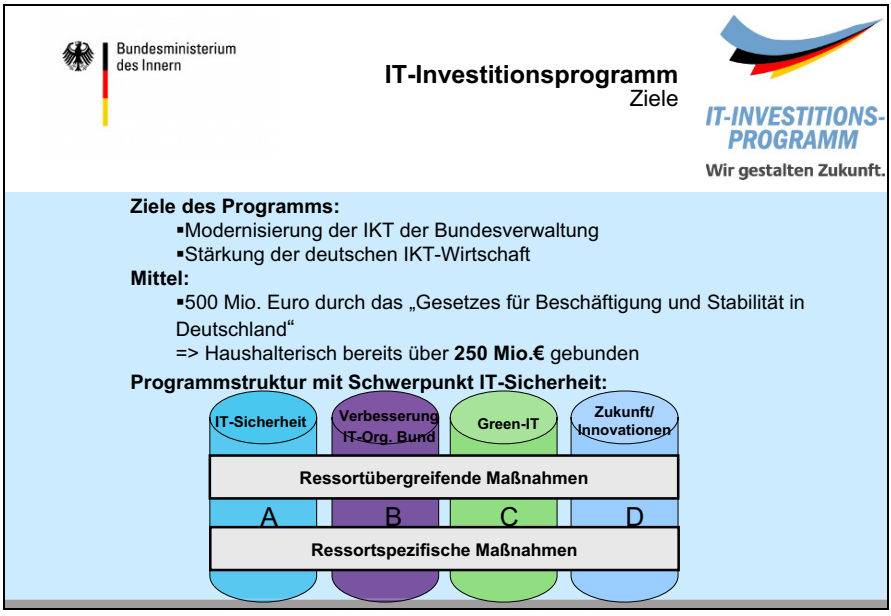


Bild 12

In der Bundesverwaltung können wir in diesem Jahr erheblich mehr in IT-Sicherheit investieren. Die Bundesregierung hat im letzten Jahr in dem Konjunkturpaket II ein milliardenschweres Programm aufgesetzt, um in der Wirtschaftskrise zu helfen, dass sich Konjunktureinbrüche in Grenzen halten. Ein Teil dieses Programms ist unter der Verantwortung der Beauftragten der Bundesregierung für Informationstechnik das IT-Investitionsprogramm (Bild 12). Der Deutsche Bundestag hat 500 Millionen Euro eingestellt, um in IT zu investieren und damit die Unternehmen in dieser Branche nachhaltig zu unterstützen. Von diesen 500 Millionen sind mit Stand Anfang d.J. 250 Millionen in den Auftragsbüchern der Unternehmen. Wir sind im Augenblick in der aktiven Phase, und ich denke, bis Mitte des Jahres werden für alle Mittel Verträge vorliegen. Ein Großteil der über 350 Maßnahmen wird bereits in

2010 zum Abschluss kommen. Aber für die Unternehmen ist es wichtig, einen staatlichen Auftrag in ihrem Auftragsbuch zu haben. Das ist das entscheidende Kriterium.

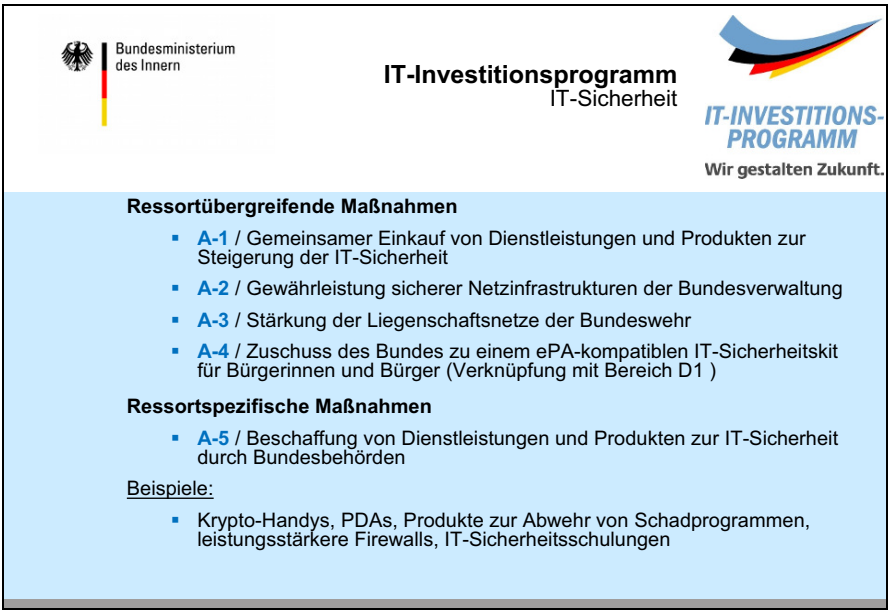


Bild 13

Im IT-Investitionsprogramm des Bundes haben wir vier Schwerpunkte gesetzt (Bild 13). Der Schwerpunkt IT-Sicherheit ist der Schwerpunkt Nummer 1. Wir haben 222 Millionen von den 500 Millionen für IT-Sicherheit veranschlagt und damit eine ganze Reihe von Investitionen bewirkt. Manches davon haben Sie vielleicht in der Presse mitbekommen. Wir haben für die Bundesverwaltung Kryptohandys erworben und auch weiterentwickeln lassen, außerdem stellen wir der Bundesverwaltung daneben sichere PDAs zur Verfügung. Wir haben eine Sensibilisierungsmaßnahme für die Beschäftigten in der Bundesregierung gestartet. Wir haben sehr viel investiert und investieren noch in die Sicherheit der Netzinfrastrukturen. Wir werden im Zusammenhang mit dem neuen Personalausweis in Kürze ein Zuwendungsverfahren starten, das helfen soll, eine größere Stückzahl Chipkartenleser auszugeben. Insgesamt stehen dafür 24 Millionen Euro zur Verfügung und wir haben die Hoffnung, dass wir damit auch eine ganz erkleckliche Anzahl von preisgünstigen Chipkartenlesern für die Erstnutzung des elektronischen Personalausweises herausbringen. Die Nachfrage, sich an diesem Programm beteiligen zu wollen, ist sehr groß und wir sind sehr hoffnungsvoll, dass es gelingen wird, die Mittel schnell zu verteilen und die Geräte auszugeben.

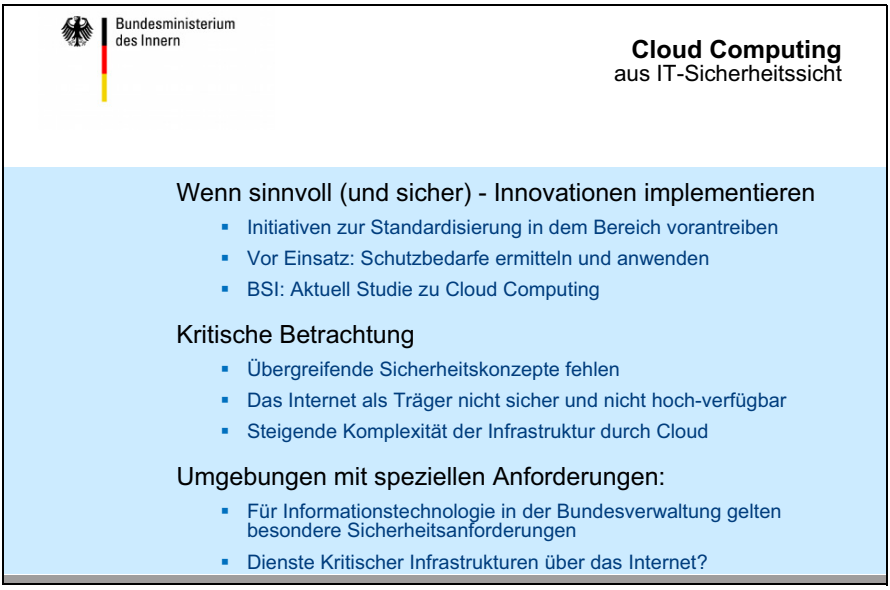


Bild 14

Zum Abschluss will ich das engere Thema dieser Veranstaltung ansprechen, auch wenn ich mich da nicht als Experte bezeichnen würde (Bild 14). Wir haben eine etwas ambivalente Einstellung zum Cloud Computing. Das BSI beschäftigt sich bereits seit einiger Zeit mit dem Thema und hat erste Bewertungen abgegeben, sich aber noch nicht abschließend festgelegt.

Standardisierung gibt es für Einzelbereiche, einzelne Komponenten, einzelne Softwarekomponenten – Herr Schwenk hat das vorgetragen. Aber es gibt keine übergreifenden Methoden oder Standards, die es zum Beispiel erlauben würden, die Verlagerung von Daten und Anwendungen aus dem eigenen abgegrenzten Netz heraus in die Cloud zu bewerten. Das BSI hat auch bereits dazu eine Studie zu Cloud Computing angestoßen, die an der Stelle helfen soll.

Ein anderes Thema, was uns natürlich besorgt macht, ist, dass mit Cloud Computing Dienste über das Internet angeboten und abgerufen werden – das Internet hat an sich dafür aber auf Grund seiner Beschaffenheit nicht die notwendigen Sicherheitsmerkmale, insbesondere die Verfügbarkeit – bereitstellen kann.

Ein anderer Aspekt, der mir wichtig erscheint, ist, dass die Anwendung von Cloud Computing eine Komplexitätssteigerung mit sich bringt. Komplexitätssteigerung ist für IT-Sicherheitsprozesse immer schwierig. Dass ein IT-Sicherheitsbeauftragter eines Unternehmens und einer Behörde durchschaut, von was genau die Sicherheit

einer Anwendung abhängt, wird sozusagen von Iterationsstufe zu Iterationsstufe immer schwieriger. Cloud Computing wird zu dieser problematischen Entwicklung nach meiner Einschätzung beitragen. Die Komplexität ist schon heute schwierig in den Griff zu bekommen. Das macht mir am meisten Sorgen. Am Ende sind Menschen verantwortlich in den Unternehmen, IT-Verantwortliche und ihre Sicherheitsbeauftragten, die durchschauen müssen, wovon eigentlich ein kritischer Geschäftsprozess abhängt.

Deshalb ein großes Fragezeichen bei dem letzten Punkt: Dienste kritischer Infrastrukturen über das Internet. Bislang sehen wir keine Entwicklung in diese Richtung. Wir treten dazu in einen Dialog mit den Betreibern kritischer Infrastrukturen. Wenn man Cloud Computing nutzen will, jedenfalls sogenannte Public Cloud-Dienste, müsste man die Kommunikation über das Internet abwickeln. Das können wir uns für kritische Prozesse und Anwendungen nicht vorstellen, ebenso wenig, wie wir uns vorstellen können, dass die Bundesverwaltung solche Public Clouds nutzt. Das einzige, was wir konkret vorbereiten, ist, dass wir im Rahmen der Konsolidierung der Rechenzentren des Bundes darüber nachdenken, ob wir sozusagen eine Private-Cloud-Struktur für die Bundesbehörden innerhalb unserer sicheren Netze aufbauen. Weiter wollen wir nicht gehen.

8 Management und Versicherung von Risiken der Informationstechnologie

Andreas Schlayer
Munich Re, München

Ich bin sehr froh, dass ich die Gelegenheit erhalten habe, Ihnen im Rahmen dieser Veranstaltung die Aspekte des Managements und der Versicherbarkeit von IT Risiken vorstellen zu dürfen. Eine Frage, die sich bei diesem Thema stellt ist: Ersetzt Versicherung Risikomanagement? Um diese Frage zu klären, möchte ich auf einem eher abstrakten Level diesen allgemeingültigen Risikomanagementprozess darstellen, anschließend exemplarisch die Möglichkeiten des Risikotransfers in Form der Sach- und Haftpflichtversicherung skizzieren und zum Schluss noch ein aktuelles Schadenbeispiel vorstellen, das es in die Weltpresse geschafft hat.

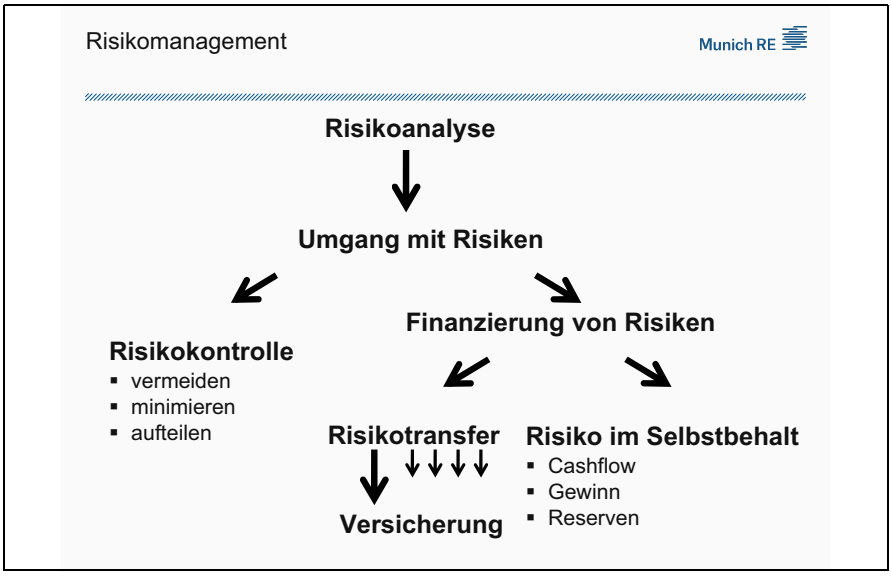


Bild 1

Betrachtet man diesen Prozess, stellt man fest, dass Versicherung ein Bestandteil des Risikomanagements ist und in keinster Weise als Ersatz oder Substitut geeignet ist.

A. Picot et al. (eds.), *Trust in IT*, DOI 10.1007/978-3-642-18110-8_8,

Der erste Schritt ist die Risikoanalyse (Bild 1). Hier ist zu entscheiden, welche Risiken betrachtet werden. Die Analysetiefe und die Anzahl der betrachteten Risiken ist durch die Menge der verfügbaren finanziellen Mittel begrenzt. Innerhalb des RM-Prozesses werden identifizierte Risiken einzeln betrachtet. Als nächster Schritt ist zu klären, wie mit einem identifizierten Risiko umgegangen wird. Hierbei gibt es zwei wesentliche Aspekte: Der eine ist die Risikokontrolle, hierunter fallen z.B. Datensicherung, Firewalls, usw. und der andere die Risikofinanzierung. Risikofinanzierung beinhaltet den Risikotransfer – die Versicherungslösung – und den „Selbstbehalt" des Risikos – was im Sinne von selber behalten zu verstehen ist. Hierbei handelt es sich um die Selbstfinanzierung des Risikos durch das Unternehmen. Dies beinhaltet alle Unternehmens- oder Unternehmerrisiken, für die kein Versicherungsschutz gekauft wird oder gekauft werden kann. Anders ausgedrückt es geht um Risikofinanzierung aus Eigenmitteln.

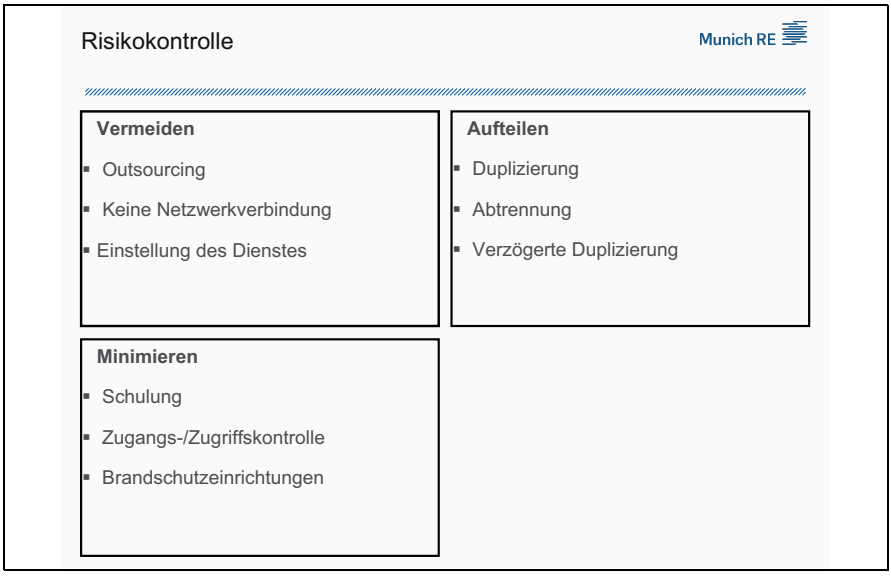


Bild 2

Als nächstes möchte ich etwas mehr ins Detail gehen und den Punkt Risikokontrolle näher betrachten (Bild 2). Risiken lassen sich durch Vermeiden, Aufteilen und Minimieren reduzieren.

Ein radikaler Schritt der Vermeidung von Netzwerkrisiken wäre eine ausschließliche Offline-Datenverarbeitung, etwas weniger radikal ist das Einstellen gewisser IT-Dienste oder Dienstleistungen. Ich möchte den Punkt Outsourcing besonders erwähnen, da hier Cloud-Computing als Maßnahme zur Risikovermeidung durchaus geeignet ist, diese Maßnahme zur Risikovermeidung möglicherweise aber

auch eine Risikoerhöhung an anderer Stelle bewirken kann. Die Antwort auf die Frage, für welche Lösung man sich entscheidet, hängt davon ab, was unter Wirtschaftlichkeitsgesichtspunkten den meisten Sinn macht. Welches Risiko schwerer wiegt, sollte im Idealfall als Ergebnis der Risikoanalyse vorliegen. Eine vernünftige Risikoanalyse wird nie ohne eine gesamtheitliche Betrachtung des Unternehmens ablaufen können.

Eine zweite Möglichkeit der Risikokontrolle ist die Aufteilung des Risikos. Diesen Ansatz findet man im IT Bereich recht häufig, indem Server auf mehrere Räume oder Standorte aufgeteilt werden. Unter Minimierung subsumiert man alle Maßnahmen zur Schadenverminderung, wie Sprinkler, CO_2-Löschanlagen im Rechenzentrum, Schulung der Mitarbeiter, Zugriffskontrollen, Firewalls, Virenscanner und sonstige Maßnahmen, die dazu dienen, das Risiko zu vermindern.

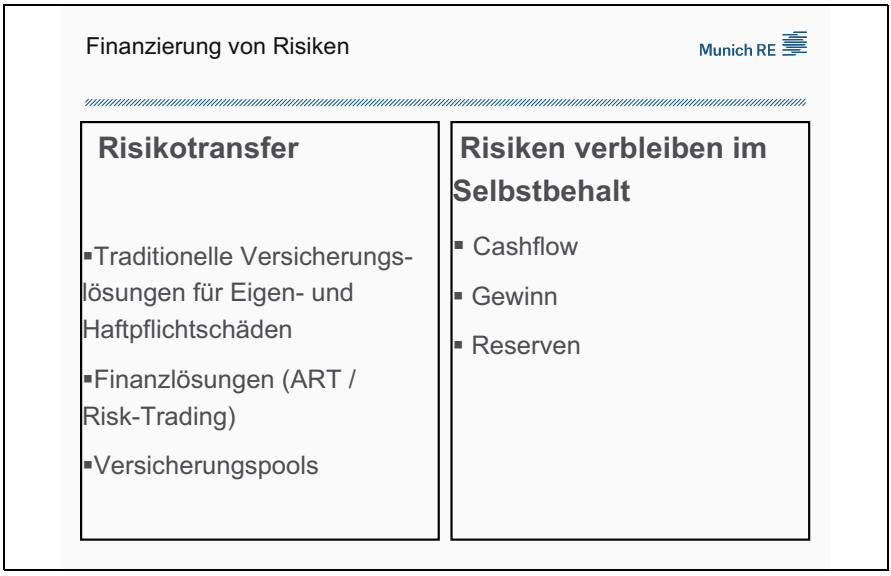


Bild 3

Risikotransfer und Risiken im Selbstbehalt

Risikotransferlösungen kennt jeder von Ihnen (Bild 3). Es handelt sich um traditionelle Versicherungslösungen wie Haftpflichtversicherung, Feuerversicherung, Hausratversicherung und zusätzlich noch Möglichkeiten wie Alternative Risk Transfer Lösungen (ART), um Risiken an den Kapitalmarkt zu verkaufen. Versicherungspools kommen eher zum Einsatz, wenn es sich um sehr große Risiken handelt, die für einzelne Versicherungsunternehmen nicht mehr ausgleichbar sind. Am häufigsten kommen Poollösungen für die Versicherung von Terrorismusrisiken

zum Einsatz. In Deutschland sowie in den USA und vielen anderen Ländern gibt es einen Versicherungspool für Terrorismus mit staatlicher Beteiligung, um ausreichend viel Kapazität für die Versicherung von Terrorismusschäden zur Verfügung stellen zu können.

Risiken verbleiben im Selbstbehalt

Das bedeutet, dass ein Risiko, welches sich realisiert hat – der Versicherer redet hier vom Schaden – aus Eigenmitteln bestritten werden muss. Ein Beispiel: Wenn Sie eine Vollkaskoversicherung haben, wird der Schaden über €150 oder 300 € von der Versicherung beglichen, der darunter von Ihnen selbst. Sozusagen ihr Selbstbehalt. Um den Selbstbehalt finanzieren zu können, müssen Sie einen möglichen Schaden durch Ihren Cashflow finanzieren, ein Stück vom Jahresgewinn opfern oder eine Reserve bilden. Kleinere Schäden, die im Selbstbehalt des Unternehmens verbleiben, werden aus dem Jahresgewinn oder Cashflow bestritten. Bei größeren Risiken, die bilanzwirksam sind, ist es ratsam sich mit einer Rückstellung aktiv auf einen möglichen Schaden vorzubereiten.

Bild 4

Wenn wir etwas tiefer in den Bereich Versicherungen einsteigen, gibt es zwei wesentliche Bereiche: Den Eigenschaden und den Drittschaden auch Haftpflichtschaden genannt (Bild 4). Im Bereich von IT Risiken führt ein Ereignis oft gleichzeitig zu einem Eigen- und einem Drittschaden. In Märkten wie den USA haben sich Versicherungsprodukte für IT-Risiken etabliert, die sowohl eine Eigenschaden- wie

auch eine Drittschadendeckung bieten. Für den Fall, dass Ihr Unternehmen vertrauliche Kundendaten verliert, gilt: Sie haben forensische Kosten und Ansprüche Dritter, die Sie decken müssen.

Die Versicherungsindustrie sieht den Eigenschaden als Schaden, den Sie als Unternehmer oder Privatperson erleiden und den das Versicherungsunternehmen ihnen entschädigt. Ich habe hier Feuer, Hochwasser, Blitzschlag aufgeführt. Drittschaden ist der Schaden, den Sie jemand anderem zufügen. Im professionellen Bereich sind das Schäden Ihrer Kunden, die diese durch Ihre Produkte oder Dienstleistungen erleiden. Im Privatbereich ist das zum Beispiel, wenn Ihr Sohn oder Ihre Tochter mit dem Fußball das Fenster eines Nachbarn einschießt, mit dem Rad an einem fremden Auto hängenbleibt oder wenn die wertvolle Vase der Tante zu Bruch geht.

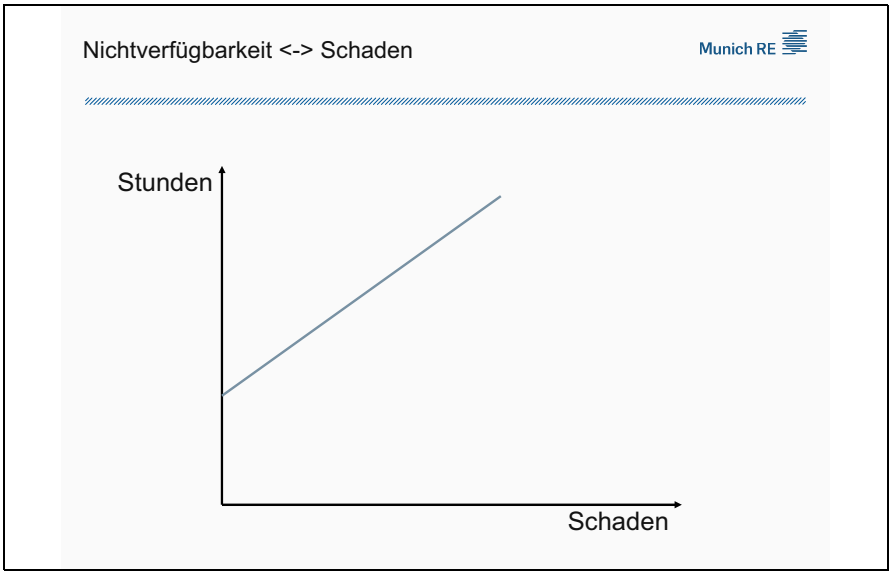


Bild 5

Dritt- und Eigenschäden können auch aus einer Unterbrechung des Geschäftsbetriebs entstehen. Zu beachten ist, nicht jede Unterbrechung verursacht automatisch einen Schaden. Abhängig davon welche Applikation, welcher Service getroffen ist, kann man unter Umständen eine gewisse Zeit darauf verzichten, ohne einen finanziellen Schaden zu erleiden (Bild 5). Wenn aber Ihr Einkaufssystem, das die Bestellungen Ihrer Kunden annimmt offline ist, bei Amazon die Homepage ausfällt oder bei eBay die Versteigerungen nicht mehr funktionieren, dann ist die Zeitspanne zwischen Ausfall und finanziellem Schaden relativ kurz. Cloud-Computing bewirkt hier einen Veränderung der Risikolage. Ohne – ist es Ihre IT-Applikation, Ihr IT-Service, Ihr Server, der ausgefallen ist und Ihre IT Abteilung ist zuständig, die Störung des

Geschäftsbetriebs möglichst schnell zu beheben. Mit – besteht eine Abhängigkeit nach außen und Sie sind vollständig abhängig von Ihrem Provider und haben wenig bis keinen Einfluss auf die Behebung der Unterbrechung. Diesen Umstand sollte man bei der Betrachtung des Unterbrechungsrisikos berücksichtigen.

Cloud-Computing kann aber auch dazu dienen, das Unterbrechungsrisiko zu minimieren, wenn es z.B. für den Serviceprovider sehr viel einfacher ist, mit redundanter Hardware oder mehreren Standorten zu arbeiten, als Sie das wirtschaftlich in Ihrem Unternehmen bewerkstelligen können. Es hat unter Umständen auch zur Folge, dass plötzlich Ihre Internetverbindung oder die Netzwerkverbindung zum Provider zu einem Flaschenhals wird.

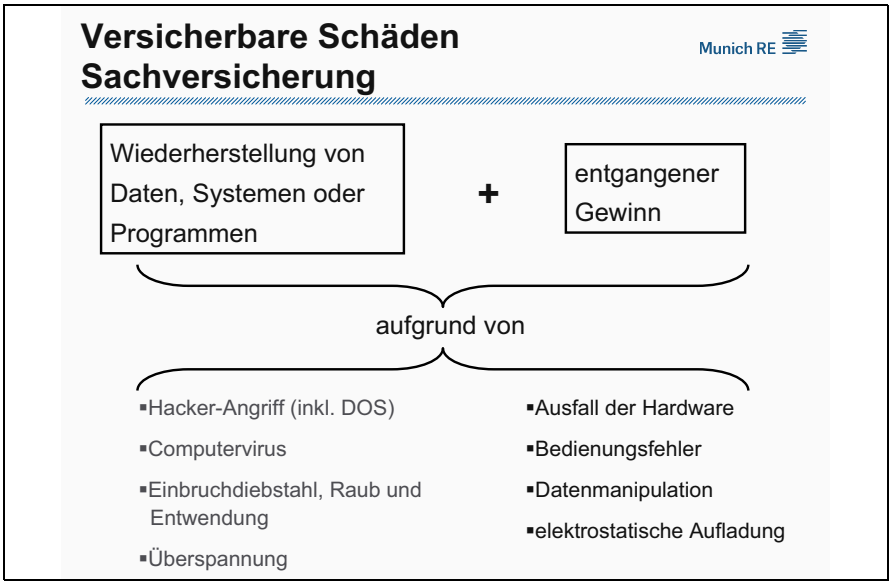


Bild 6

Was im Rahmen der Sachversicherung versichert wird, sind die Wiederherstellungskosten für Daten und Programme und der Gewinn, der dem Unternehmen bei Verlust dieser entgeht (Bild 6). Versicherbare Schäden sind Hackerangriffe und Computerviren; ebenfalls versicherbar ist Einbruchsdiebstahl, Raub und Entwendung, z.B. der Diebstahl einer Festplatte mit wertvollen Daten. Wie wir in einem der vorherigen Vorträge gehört haben, ist man in Deutschland als Unternehmen verpflichtet die Personen zu benachrichtigen, deren vertrauliche Daten möglicherweise Dritten zugänglich wurden. Die entstandenen Kosten für das Benachrichtigen der betroffenen Personen können versichert werden. Bei einer sehr großen Anzahl betroffener Personen können hier durchaus erhebliche Kosten entstehen. Ausfall der Hardware, Überspannung, Bedienungsfehler, Datenmanipulation und elektrostatische Aufladung

sind weitere häufige Ursachen für Schäden.

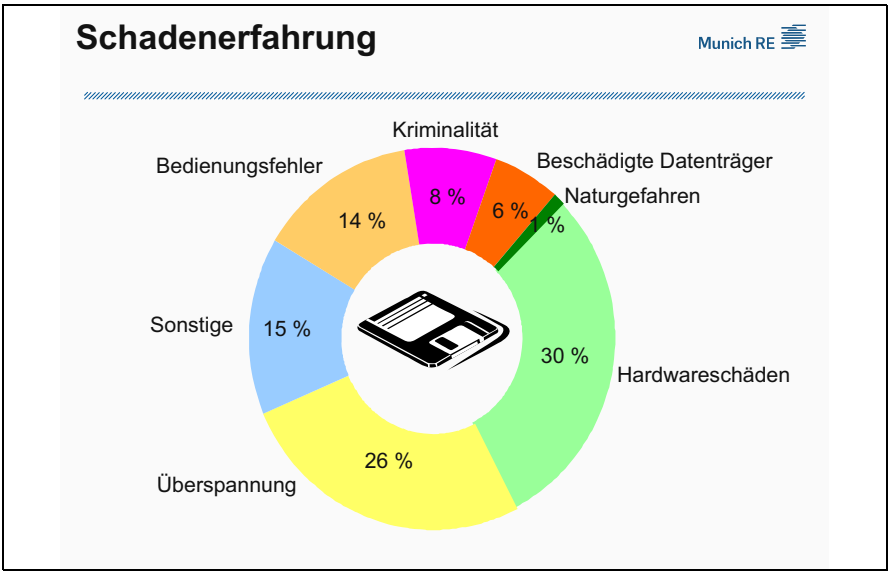


Bild 7

Ich habe Ihnen eine Schadenstatistik aus dem deutschen Markt mitgebracht (Bild 7). Das Interessante daran ist, dass die Zusammensetzung der Schäden, die der Versicherungsindustrie in diesem Bereich gemeldet wurden, nicht gänzlich die Schadenerfahrung der versicherten Unternehmen widerspiegelt. Für Hardwareschäden und Überspannung ist die Statistik relativ scharf. Bei Schäden, die aus dem Bereich Kriminalität gemeldet wurden, handelt es sich meist um Diebstahl von Hardware. Beschädigte Datenträger sind heute auch nicht mehr so das Thema.

Bedienungsfehler und sonstige Schadenursachen: Ich gehe davon aus, dass sich der Anteil hier in Zukunft weiter erhöhen wird. Man subsumiert hier Schäden durch Benachrichtigungskosten, Kosten für forensische Untersuchungen, Datenrekonstruktion und daraus resultierende Unterbrechungsschäden. Eine Erkenntnis, die wir aus Rückfragen bei Unternehmen gezogen haben, ist, dass viele Unterbrechungsschäden – obwohl vielleicht sogar Versicherungsschutz bestanden hätte – mangels geeigneter Controllingprozesse aus den IT-Budget bestritten werden und damit unnötigerweise den Gewinn des Unternehmens vermindern.

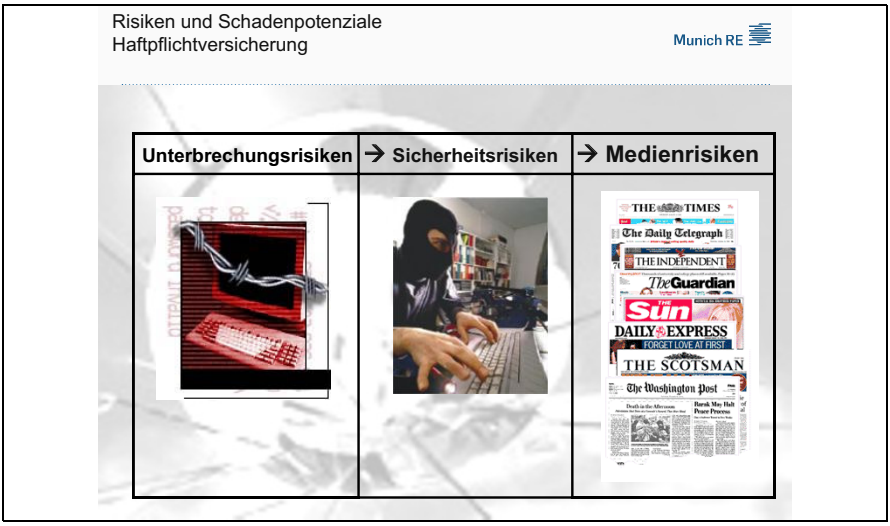


Bild 8

Die Haftpflichtversicherung deckt finanzielle Schäden ab, die eine Person einer anderen Person zufügt. Die größten Gefahren für Anbieter von Cloud-Computing-Dienstleistungen gehen von Unterbrechungsrisiken und Sicherheitsrisiken aus, die zu finanziellen Schäden bei ihren Kunden führen können (Bild 8). Bei Medienrisiken hatten wir in der Vergangenheit, Anfang der 2000er Jahre, große Schäden. Die meisten davon wurden durch die Verletzung des Urheberrechts verursacht. Seit 3-4 Jahren sehen wir zunehmend mehr Schäden aus Sicherheitsrisiken; hier ist ein klarer Trend festzustellen.

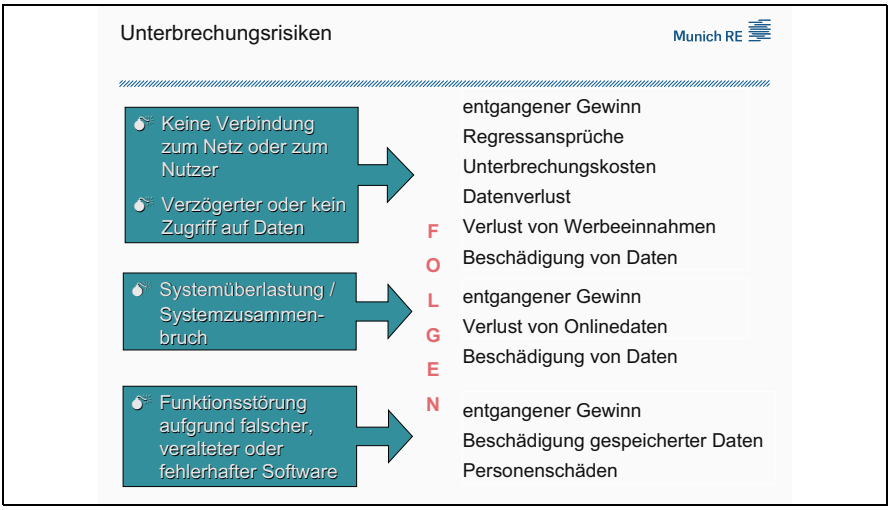


Bild 9

Mit Unterbrechungsrisiko bezeichnet man das Risiko, dass eine Netzwerkverbindung oder ein anderer wichtiger Service eines Unternehmens ausfällt und dadurch der Geschäftsbetrieb beeinträchtigt ist (Bild 9). Wenn diesem Unternehmen durch Verschulden des Providers Gewinn entgeht oder Kosten entstehen, kann das zu Regressansprüchen führen. Gleiches gilt auch für Datenverlust, Verlust von Werbeeinnahmen, Beschädigung von Daten.

Systemüberlastung und Systemzusammenbruch kann auch ein Grund sein für einen Regressanspruch, genauso wie Funktionsstörung, falsche und fehlerhafte Software. Es gibt spezielle Versicherungsprodukte, die Entwicklungsrisiken von Software abdecken. Wie z.B. Sicherheitslücken in Ihrer Software, die wiederum bei Ihrem Kunden dazu führen können, dass Hacker Zugang zu diesen Systemen erlangen und vertrauliche Daten entwenden.

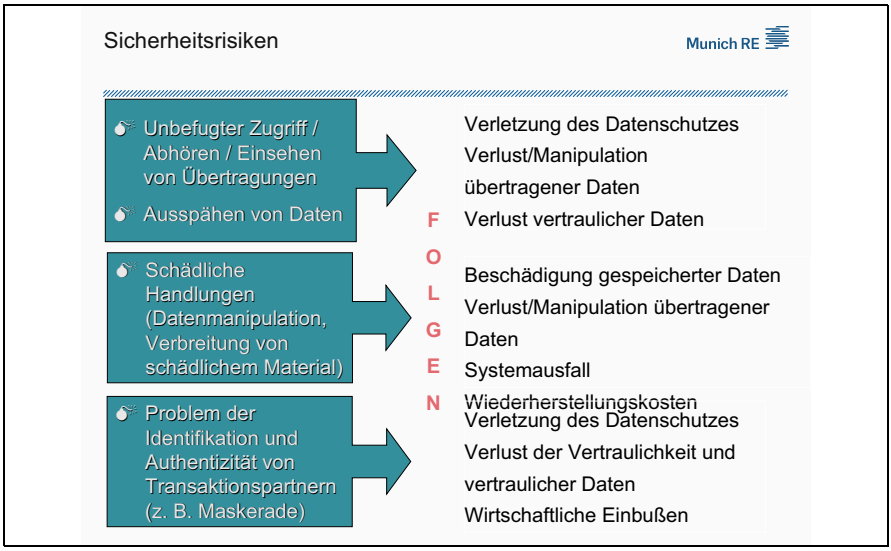


Bild 10

Sicherheitsrisiken, wie vorhin erwähnt, sind zur Zeit diejenigen, welche die größten und prominentesten Schäden verursachen (Bild 10). Die Verletzung des Datenschutzes ist momentan eine der häufigsten Gründe für sehr große Schäden. Wenn ein Hacker unberechtigt Zugriff auf ein System erlangt, vertrauliche Daten aus diesem System kopiert – sehr beliebt sind Kreditkarten – und an Dritte verkauft, verlangt der Gesetzgeber in Deutschland seit September 2009, in den USA schon etwas länger, dass die „Besitzer“ dieser Datensätze benachrichtigt werden müssen. Wenn diesen „Besitzern“ Kosten aufgrund Missbrauch dieser Daten entstehen – wie betrügerische Abhebungen von Geld oder Einkäufe mit geklauten Kreditkartendaten – müssen diese Kosten ebenfalls ersetzt werden.

Gerade bei den Kreditkarten kommt es zunehmend mehr zu Schadensersatzansprüchen von den Banken, diese möchten einen Teil der Kosten für kriminelle Transaktionen und Neuausstellung der Kreditkarten von den Firmen, denen die Daten gestohlen wurden, ersetzt bekommen.

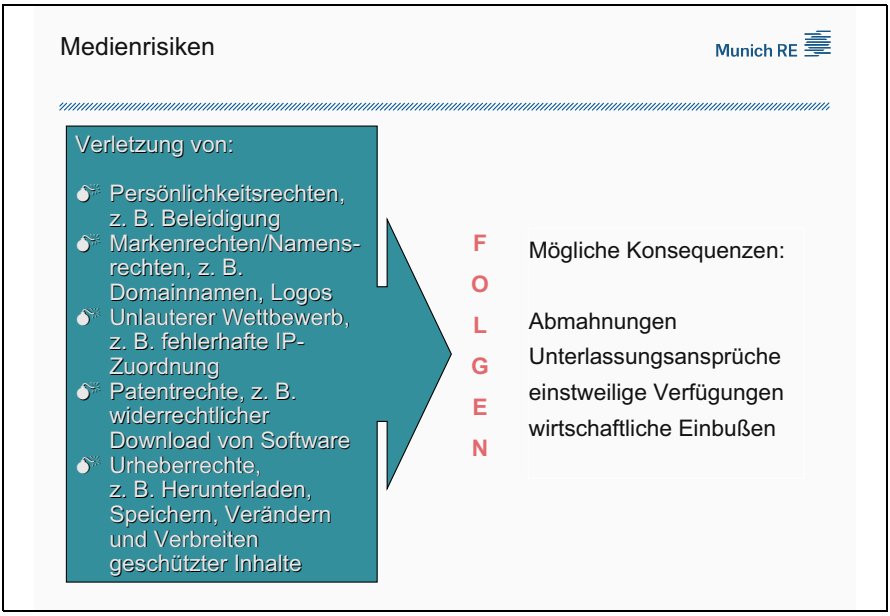


Bild 11

Bei Medienrisiken sahen wir die meisten Schäden Anfang der 2000er Jahre mit Medieninhalten (Fotos, Musik, Filme aber auch Markennamen), die im Internet veröffentlicht oder verwendet wurden, ohne die Verwertungsrechte zu besitzen oder die Copyrightansprüche abgeklärt zu haben (Bild 11). Urheberrechtsgeschützte Inhalte können übers Internet sehr schnell verbreitet werden. Anwaltskanzleien oder spezielle Serviceunternehmen haben sich darauf spezialisiert, nach Urheberrechtsverstößen zu recherchieren, diese gezielt abzumahnen und ggf. Schadenersatzansprüche geltend zu machen. Es gab auch einige Schäden, bei denen gegen Softwarepatente verstoßen wurde, wie z.B. dem 1-Click Patent von Amazon.

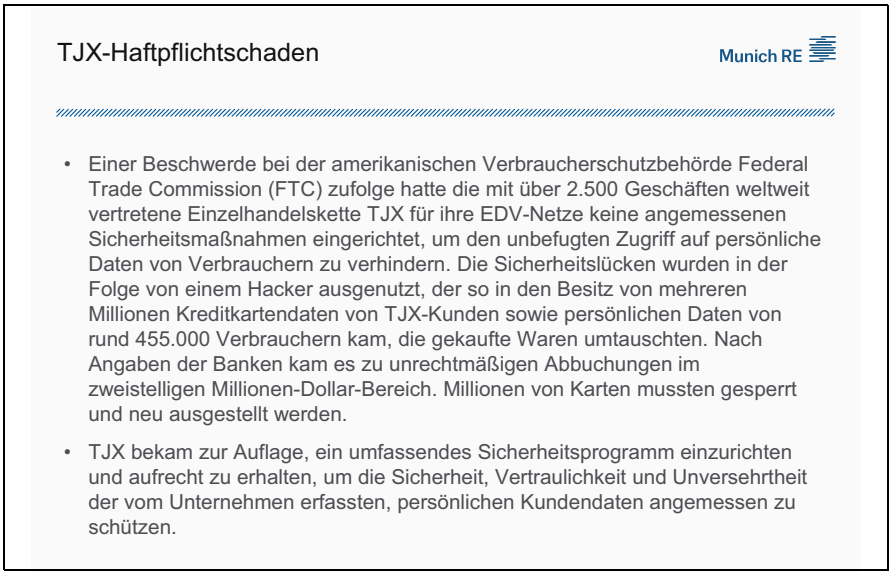


Bild 12

Zum Ende meines Vortrages möchte ich noch auf ein prominentes Schadenbeispiel eingehen. Einer der größten Schäden, den die Versicherungsbranche im Bereich der Informationstechnologie regulieren musste, ist bei TJX, einer großen amerikanischen Supermarktkette eingetreten (Bild 12). Einer Beschwerde bei der amerikanischen Verbraucherschutzbehörde Federal Trade Commission (FTC) zufolge, hatte die mit über 2.500 Geschäften weltweit vertretene Einzelhandelskette TJX für ihre EDV-Netze keine angemessenen Sicherheitsmaßnahmen eingerichtet, um den unbefugten Zugriff auf persönliche Daten von Verbrauchern zu verhindern. Die Sicherheitslücken wurden in der Folge von einem Hacker ausgenutzt, der so in den Besitz von mehreren Millionen Kreditkartendaten von TJX-Kunden sowie persönlichen Daten von rund 455.000 Verbrauchern kam, die gekaufte Waren umtauschten. Nach Angaben der Banken kam es zu unrechtmäßigen Abbuchungen im zweistelligen Millionen-Dollar-Bereich. Millionen von Karten mussten gesperrt und neu ausgestellt werden. TJX bekam zur Auflage, ein umfassendes Sicherheitsprogramm einzurichten und aufrechtzuerhalten, um die Sicherheit, Vertraulichkeit und Unversehrtheit der vom Unternehmen erfassten, persönlichen Kundendaten angemessen zu schützen. Der Schaden belief sich auf ca. 150 Millionen Dollar.

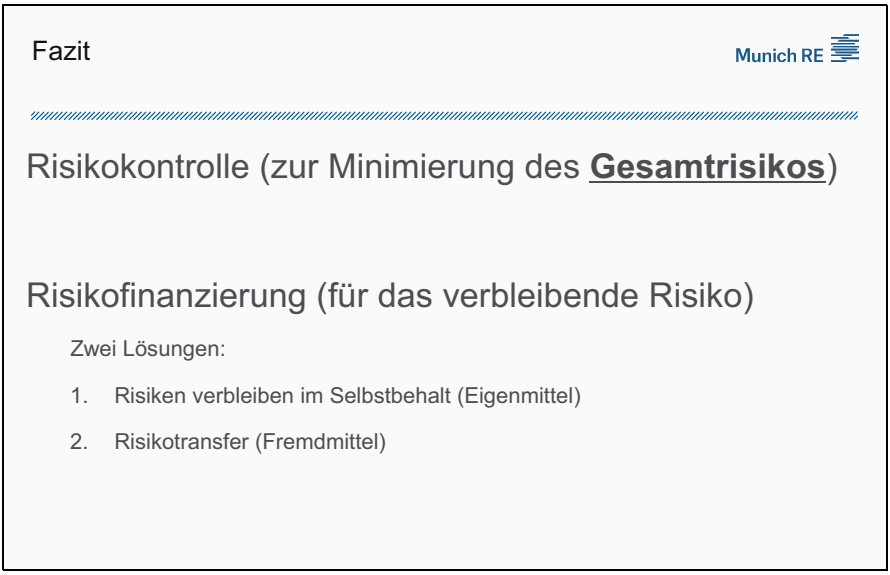


Bild 13

Zum Abschluss möchte ich ein kurzes Fazit ziehen (Bild 13). Die Risikokontrolle dient dazu, das Gesamtrisiko im Unternehmen zu minimieren. Die Entscheidung, welcher Weg der Risikofinanzierung gewählt wird, sollte unter wirtschaftlichen und Haftungsgesichtspunkten getroffen werden. Hierbei ist zu beachten, dass Risiken, die eine niedrige Frequenz und eine hohe Intensität haben, über eine Versicherungslösung günstiger finanzierbar sind als über Eigenmittel. Wenn es sich um Risiken handelt, die eine hohe Frequenz und eine niedrige Intensität haben, wird sich eine Versicherungslösung nicht lohnen. Eine Verbesserung der Risikokontrollen und eine Finanzierung mit Eigenmitteln ist für solche Risiken die wirtschaftlichere Lösung.

9 Neue IT-Dienste: Zwischen Rationalisierungspotential und Kontrollverlust

Prof. Dr. Günter Müller
Institut für Informatik u. Gesellschaft, Universität Freiburg

Wenn wir neue IT-Dienste angehen, zu denen auch Cloud Computing gehört, haben wir ein ganz einfaches Geschäftsmodell. Das Geschäftsmodell heißt immer: Sie geben mir Ihre Daten und ich gebe Ihnen tolle Dienste. Diese Dienste haben aber ökonomische Konsequenzen, die manchen nicht so klar sind. Ich werde es an drei Dingen zeigen:

Zum Einen haben wir Kontrollverlust: Meine These ist, dass unser Datenschutzgesetz einfach ein Gesetz ist, das eine Technologie vor 30 Jahren im Auge hat. Informelle Selbstbestimmung ist aber ein Grundrecht. Es kann nicht aufgegeben werden, es muss vielmehr mit guten Mechanismen ermöglicht werden.

Zum Zweiten, die ökonomische Vorteile: Hierzu sollten wir das Problem aus der Sicht der Nutzer und der Anbieter sehen. Die Nutzer sind verkettet und haben Zugang zu allen Daten und die kostenlos. Die Anbieter werden sich konzentrieren und einen neuen Ort für das Computing an sich finden. Nicht mehr die maßgeschneiderte Lösung beim Kunden, sondern die Bereitstellung der gewünschten Ergebnisse durch den Anbieter wird die Lösung der Zukunft sein.

Drittens ist man nicht chancenlos den Sachzwängen der neuen Dienste ausgeliefert. Am Ende werde ich auf Lösungen eingehen, die wir in Freiburg aber in der Wissenschaft auch anderswo bearbeiten, und Cloud verspricht es uns auch.

A. Picot et al. (eds.), *Trust in IT*, DOI 10.1007/978-3-642-18110-8_9,

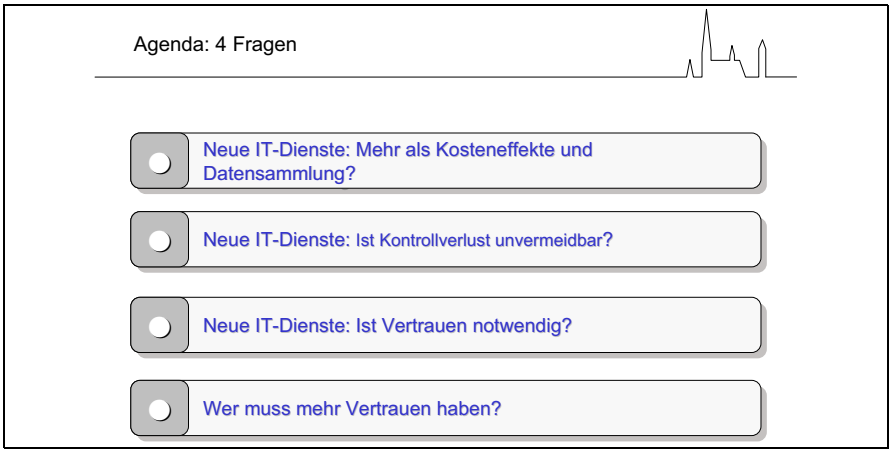


Bild 1

Ich werde meine Argumente in vier Schritten vortragen (Bild 1): Diese neuen IT Dienste sind mehr als Kosteneffekte und Datensammlungen. Bei den neuen IT Diensten ist Kontrollverlust unvermeidbar. Jemand hat behauptet, dass die Privatsphäre ein Fehlurteil der Zivilisation sein und es sich in der Evolution herausgestellt habe, dass die Menschheit das gar nicht braucht. Die letzten beiden Punkte beschäftigen sich also mit Vertrauen. Das ist vielleicht gesellschaftlich die interessantere Frage.

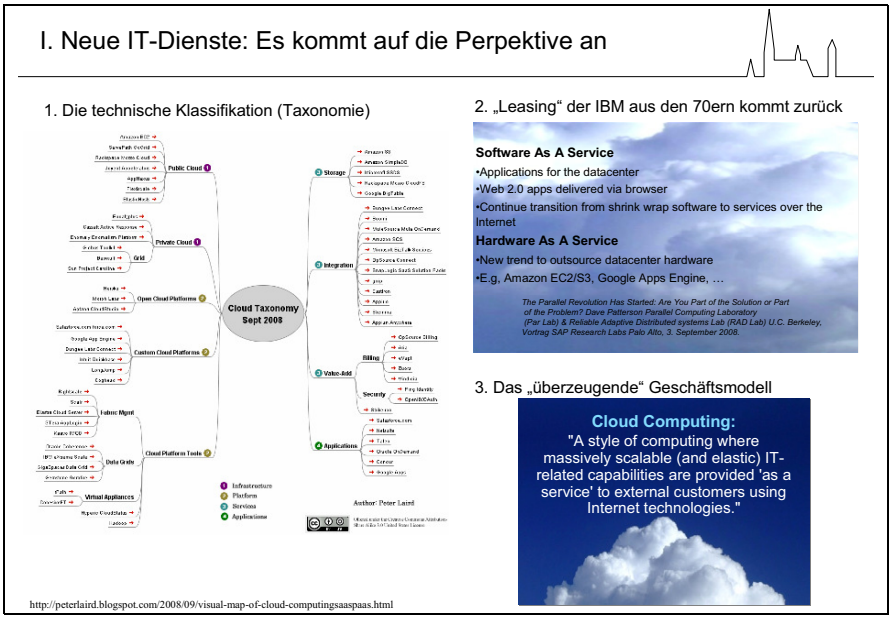


Bild 2

Auch Computing hat eine Geschichte (Bild 2). Heute heißt die aktuelle Variante „Cloud Computing“ und das Versprechen ist, dass alles deutlich billiger wird. Das Geschäftsmodell der IBM in den 70er bis 90er Jahre war, dass Hardware verkauft wurde. D.h.man hat nicht verkauft, sondern vermietet. Dann ist irgendeiner darauf gekommen, dass bei der Wertschöpfungskette Hardware gar nicht das Entscheidende ist sondern vielleicht die Software. Dann sind so etwas wie die SAP und Oracle gekommen. Wenn wir noch ein Stück weitergehen, stehen wir vor der Frage, warum wir auch noch diese Dienste irgendwo einkaufen sollen und teures Geld für Customizing zahlen sollen. Dies wird nun technisch möglich durch eine Ansammlung von Rechnern, die lose miteinander verbunden sind und die man heute als „Cloud“ oder „Wolke“ bezeichnet. Cloud ist mehr als ein Netzwerk oder Cluster. Die Knoten können sich helfen. Dazu haben wir seit September 2008 eine technische Klassifikation. Der nächste Teil der Folie geht schon auf die Verendung ein. Das neue Geschäftsmodell heißt „Software as a Service“. Im dritten Teil der Folien wird es nebulöser, aber eigentlich sogar deutlicher. Wir bekommen eine neue Form des Computing – das Cloud Computing, und das wird extrem viel billiger werden und die Wirtschaft und die Privatpersonen werden nicht mehr zu hause oder im Betrieb rechnen, sondern Computing nach Bedarf anmieten, wie dies beim privaten E-mail Account beim Anbieter schon heute der Fall ist. Hätte man sich diese Selbstverständlichkeit vor 5 Jahren vorstellen können? Cloud ist nicht IT oder Informatik. Es ist ein „Lebensstil“. Wer von den IT Providern das hinbekommt, der verdient Geld. Wer das nicht hinbekommt, verdient nichts und wird aus dem Markt ausscheiden. Aber auch die Privatleute werden bei aller scheinbaren Kostenlosigkeit zahlen müssen. Es ist nichts umsonst, nur die Währung wird die Privatsphäre sein.

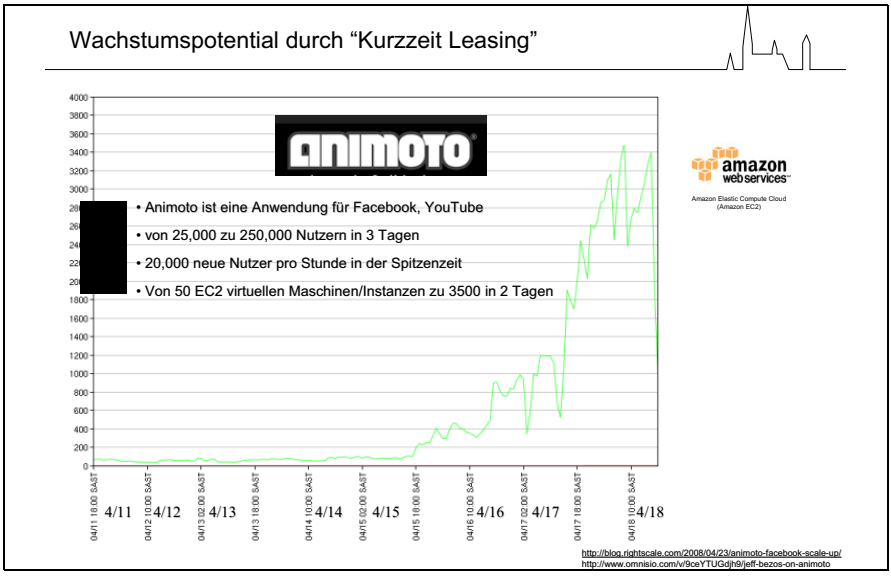


Bild 3

Die Rationalisierungsfirma Animoto gehört zu Amazon (Bild 3). Diese Firma Animoto hat dadurch, dass sie beim Amazon Cloud mieten konnte, sich dem Markt anpassen können. Das ist eine Anwendung von Facebook und YouTube. Sie ist innerhalb von drei Tagen von 25.000 auf 250.000 Nutzer gestiegen. Sie hat 20.000 neue Nutzer pro Stunde dazu bekommen. Sie ist von 50 virtuellen Maschinen auf 3.500 in zwei Tagen gewachsen. Das hätte keine Organisationsform des klassischen Computing oder auch kein heutiger Dienstleister anbieten können. Noch wäre das Wachstum möglich gewesen, da kein Unternehmen dazu die nötige IT hätte bereitstellen können.

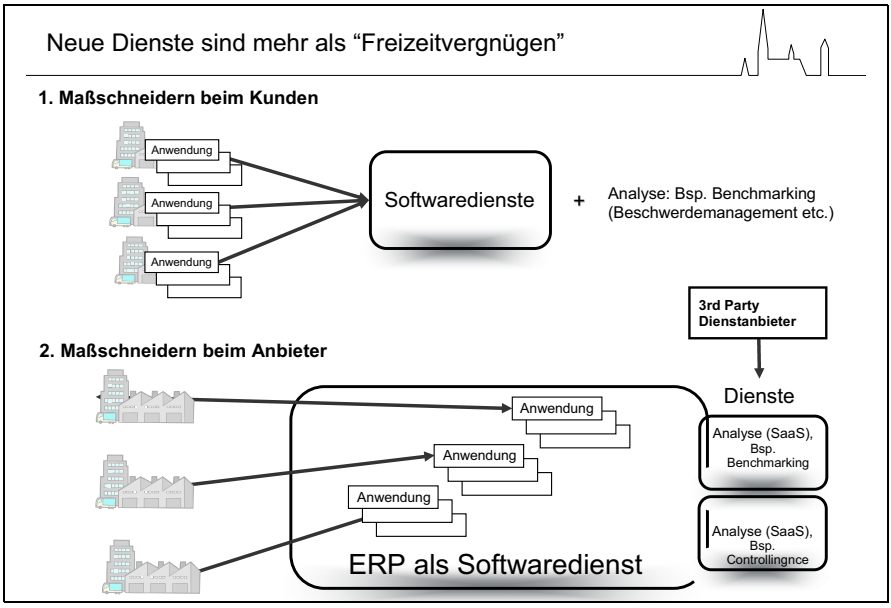


Bild 4

Ist dies nun ein wirtschaftlicher Segen und wenn ja für wen? Bisher haben wir das Geschäftsmodell, dass man für den Kunden zuschneidert (Bild 4). Dies ist im obigen Teil der Folie gezeigt und beschreibt das Vorgehen aller heutigen Berater von IM bis SAP und Oracle. Der untere Teil ist die Zukunft. Sollte es gelingen komplexe Geschäftsprozesse zu standardisieren, wird kein IT-Leiter oder CIO, mit den Kosten des Cloud mithalten können. Noch ist es nicht soweit, aber es ist eine Frage der Beherrschung von Komplexität, nicht bei der Hardware oder Betriebssoftware, sondern bei den Diensten.

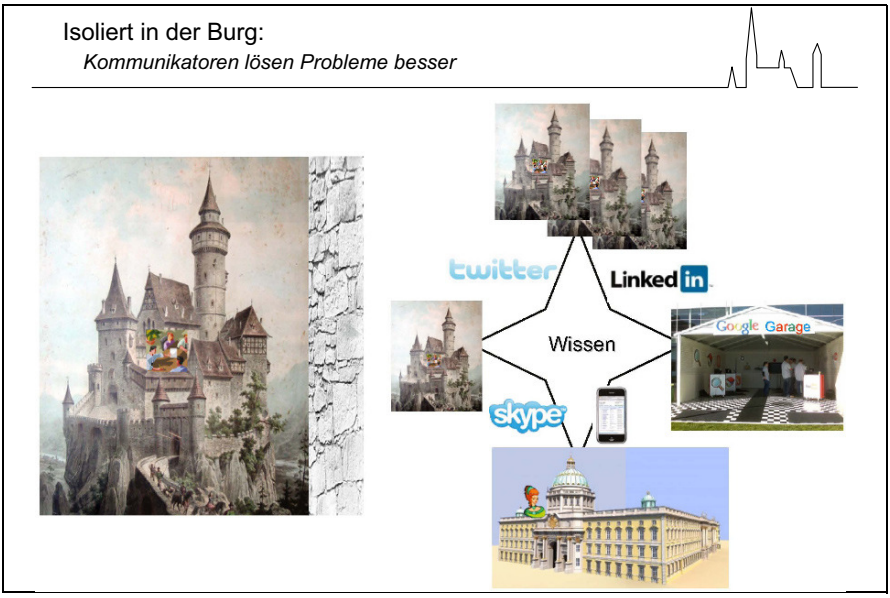


Bild 5

Hier sehen wir ein Burg und in dieser Burg – so lautet die Metapher – ist das Wissen (Bild 5). Danben sehen Sie viele kleine Burgen und die Burgen kommunizieren miteinander und erzeugen durch diese Kooperation mehr Wissen. Es ist schon heute so, dass auf diese sehr private Form des Wissensmanagements heute keine Firma verzichten kann, auch kein Student, wie ich Ihnen gesichert mitteilen kann. Er oder Sie suchen ihre Partner für die Lerngruppe mit StudiVZ oder Facebook. Die Firmen haben davor Angst und dies zu Recht. Ich habe es in Japan bei einer bekannten Elektronikfirma erlebt, die furchtbare Angst hatte, dass ihre Mitarbeiter über private soziale Netze Firmengeheimnisse verraten und Einfalltore für Spione bieten. Die Ängste kommen daher, dass in der heutigen Zeit kreative Mitarbeiter nicht nur der Firma gegenüber Loyalität haben, sondern diese Mitarbeiter sind in ein Netzwerk eingebunden. Das ist eine enorme Herausforderung für Unternehmen, aber es eröffnet neuen und günstigen Zugang zu Wissen. Man muss aber verstehen, wie man damit umgehen sollte.

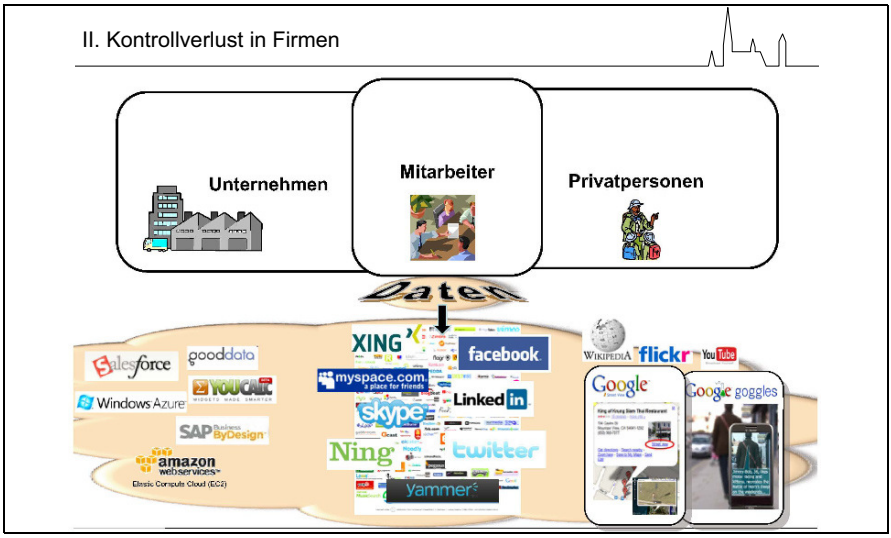


Bild 6

Diese Dienste zur Verbesserung des Wissens entmonopolisiert die Universitäten und die Firmen (Bild 6). Ich zeige Ihnen nun ein paar Beispiele, die Sie alle kennen. Myriaden von neuen Diensten entstehen. Wichtig sind wenige und überleben werden auch nur wenige. Man will ja Standards, sonst realisieren sich die Kostenvorteile nicht und die Massenvorteile entstehen nicht.

Bild 7

Hier sehen Sie die Dienste von Google, insbesondere Street View (Bild 7). Google fährt durch die Städte und fotografiert alles Mögliche. Man sagt: das macht ja nichts aus, weil mich ja keiner mit Namen identifizieren kann. Täuschen Sie sich nicht. Wenn Sie Spuren im Netz hinterlassen, weil Sie z.B. Google nutzen, wird man irgendwann ihren Namen haben. Mit Goggle werden Sie dann die Kamera Ihres Handy auf eine Person richten können und Google wird Ihnen Namen und evtl. den Lebenslauf oder sonstiges dieser Person geben.

Bild 8

Auf Grund der Gesichtserkennung sieht man, dass dieser Mann Jimmy Bob heißt, 36 Jahre alt ist und Motorradrennen mag (Bild 8). Wollen wir das? Wir können uns nicht wehren, ist meine These, solange wir Gesetze haben, die sich an der Technik von vor 30 Jahren ausrichten und solange Personen, die nicht wissen, von was sie reden, fordern, dass das Grundrecht auf informationelle Selbstbestimmung aufgegeben werden sollte, da ja jeder die Daten freiwillig hergebe, weil er der ökonomischen Theorie entsprechend seinen Nutzen selbst einschätzen könne und dies der Allgemeinheit diene.

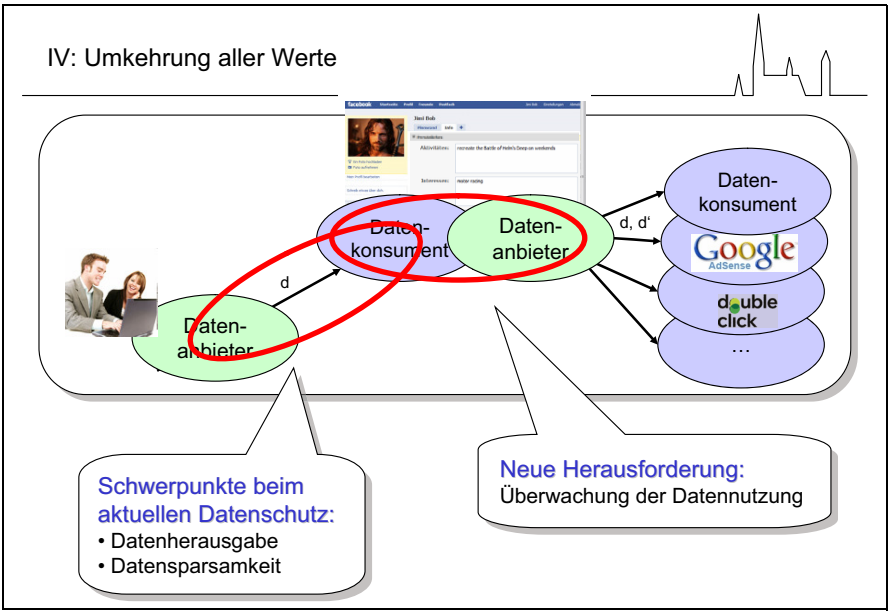


Bild 9

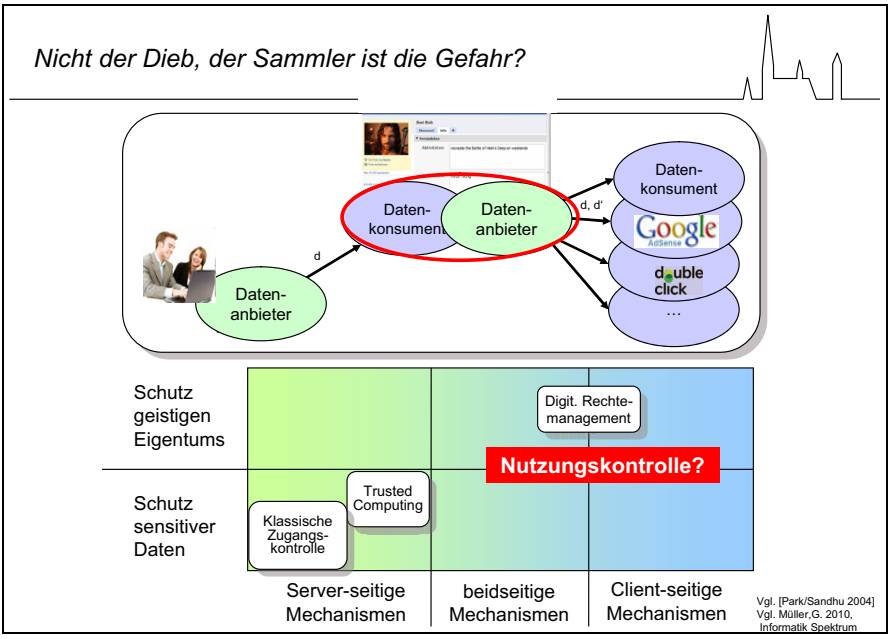


Bild 10

Wo liegt der Ansatz für einen besseren Datenschutz und die informationelle Selbstbestimmung? Google bereitet jede Information auf, weil dies im „Cloud“ unglaublich billig ist (Bild 9, Bild 10). Wie man an der MAC -Adresse kennt, ist diese Information wertvoll und wird von der Werbeindustrie nachgefragt. Also, Google speichert die IP Adressen. Die kennen Ihren Namen nicht wirklich, aber Google kann ihre Namen und ihre Aktionen herausbekommen, wie Sie aus den Beispielen sehen. Es ist ein konzeptionelles Problem. Ich nenne es die Umkehrung aller Werte. Es stammt ursprünglich von Nitzsche. Es ist nun leichter etwas zu wissen, als etwas nicht zu wissen. Lassen Sie sich das Modell erläutern, das Sie auf der Folien sehen, um zu zeigen, wo man beim Datenschutz ansetzen muss. Sie sind der Datenanbieter. Der Anbieter der neuen Dienste ist in dieser Terminologie der Datenkonsument. Bezüglich Datenschutz und Privatsphäre haben wir folgendes Problem, dass der Datenkonsument zum Datenanbieter werden könnte. Er kann die Daten falsch oder richtig weitergeben, auf jeden Fall braucht er den Datenanbieter nicht zu unterrichten, sollte der sich zuvor mit den Geschäftsbedingungen per „Click“ einverstanden erklärt haben.

Das Datenschutzgesetz, das wir haben, regelt das Verhältnis vom Datenanbieter zum Datenkonsumenten, indem wir einen Vertrag oder eine Vereinbarung über persönliche Daten schließen. Aber die Aktion und das wirtschaftliche Interesse, z.B. von Google, ist zwischen Datenkonsument und der Möglichkeit in die Rolle des Datenanbieters zu wechseln, also die gesammelten Daten zu verwerten oder zu verkaufen. Man sollte jedoch den Datenkonsumenten, der möglicherweise zum Datenanbieter wird, kontrollieren können. Und das kann man noch nicht.

Wenn wir die Technik analysieren stellen wir fest, dass wir serverseitige Mechanismen haben, die den Datenkonsumenten, also z.B. Google schützen, weil der Datenanbieter nicht auf deren gesammelte Daten zugreifen darf. Was man brauchen ist die Nutzungskontrolle.

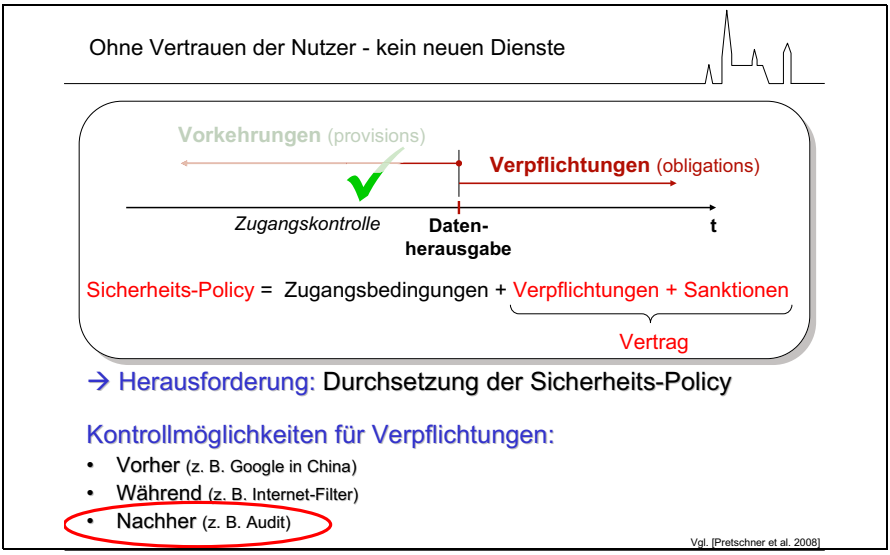


Bild 11

Was ist die Nutzungskontrolle? Es gibt den Zeitpunkt, an dem die Daten herausgegeben werden, also wenn Sie von einer Kamera im öffentlichen Raum fotografiert werden oder wenn Sie im privaten Raum eine Google Suche starten (Bild 11). Was dann sein müsste, wäre die Verpflichtung seitens dieses Datenkonsumenten, was dieser mit den Daten macht. Es ist wiederum eine Umkehrung der bekannten Werte. Nicht der Datenkonsument sollte real geschützt werden, sondern dem Datenanbieter sollte der Zugriff zu seinen Daten beim Datenkonsumenten erlaubt werden.

Die gesetzliche Herausforderung wäre eigentlich, wie wir einen Vertrag mit irgendjemand schließen können, der unsere Daten aufnimmt, von dem wir aber nicht wissen, wie er sich mit den Daten hinterher umgibt.

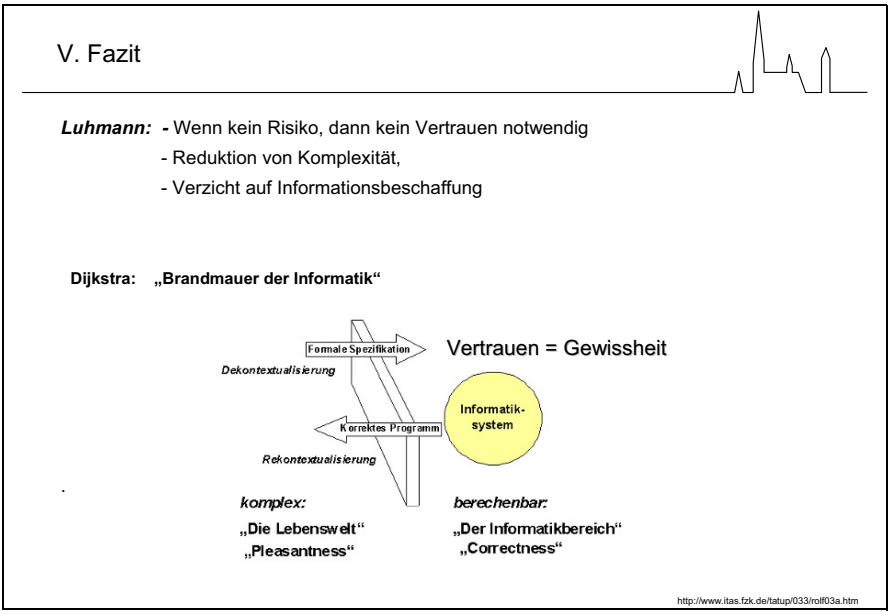


Bild 12

Das Fazit zum heutigen Thema lautet so (Bild 12): Vertrauen ist die Reduktion von Komplexität in der Gesellschaft. Man verzichtet auf Informationsbeschaffung, die man ausführen könnte, die aber zu teuer ist. Bei der IT und in der IT Industrie unterscheidet man nicht zwischen Wissen und Vertrauen. Man kennt nur Wissen, dann aber braucht es kein Vertrauen. Das Wissen, das wir haben, ist jedoch so, dass wir es real nicht wissen und daher vertrauen müssen.

Bild 13

Zum Schluss habe ich noch etwas aufgehoben, was ich Ihnen gern zeigen würde (Bild 13). Das Motto von Google ist: „Do no Evil!“ Der Schlusssatz von Mielke, dem Stasichef, war „Ich liebe doch alle Menschen“. Der CEO von Google, Herr Schmidt, soll gesagt haben: Wenn du nicht willst, dass Du in Google aufgezeichnet wirst, dann tue nichts Übles.

10 Podiumsdiskussion Wann vertrauen Sie Ihrem IT-Versorger? Cloud und Trust in der Kontroverse von Anbietern und Konsumenten

Moderation: Prof. Dr. Arnold Picot
Ludwig-Maximilians-Universität München

Teilnehmer:
Michael Auerbach, T-Systems International GmbH, Darmstadt
Prof. Dr. Gunter Dueck, IBM Deutschland GmbH, Mannheim
Kai Gutzeit, Google Germany GmbH, München
Michael Leistenschneider, DATEV eG, Nürnberg
Dr. Philipp Räther, UBS Investment Bank, London
Holger Sirtl, Microsoft Deutschland GmbH, Unterschleißheim
Dr. Peter Unkel, RWE Power AG, Essen

Prof. Picot:
Ich möchte unser Panel kurz vorstellen und gehe alphabetisch vor. Zunächst Herr Michael Auerbach. Er ist Diplom-Ingenieur, war bei EDS, einer Outsourcing Firma, tätig, beim IT Service debis Systemhaus und dann bei der T-Systems, wo er durch verschiedene Stufen in eine hohe Managementverantwortung gelangt ist. Seit kurzem ist er verantwortlich für das Global Service Delivery Management von T-Systems.

Neben ihm sitzt Herr Prof. Gunter Dueck. Herr Dueck hat Mathematik und Betriebswirtschaft studiert und verschiedene wissenschaftliche Lorbeeren erhalten, ist dann aber zu IBM gegangen und dort seitdem in der Forschung sehr engagiert tätig. Er ist Distinguished Engineer von IBM, Mitglied der IBM Academy of Technology und zugleich korrespondierendes Mitglied der Akademie der Wissenschaften in Göttingen. Er arbeitet bei IBM unter anderem auf dem für IBM und die ganze Wirtschaft sehr wichtigen Programm der Industrialisierung von Dienstleistungen, insbesondere hier IT Infrastrukturen, wozu dann auch das Cloud Computing zählt.

Dann darf ich Herrn Kai Gutzeit von Google Germany GmbH begrüßen. Er ist dort seit Anfang 2008 der Head of Google Enterprise für Deutschland, Österreich und die Schweiz, also für die unternehmensbezogenen Anwendungen von Google, sehr passend zu unserer Thematik. Bevor er zu Google kam war er bei verschiedenen Unter-

A. Picot et al. (eds.), *Trust in IT*, DOI 10.1007/978-3-642-18110-8_10,

nehmen im Bereich der Telekommunikations-, Software- und Internetindustrie tätig, auch im Ausland und in verschiedenen Funktionen in Europa. Er hat also eine breite und vor allen Dingen marktorientierte Erfahrung in dieser Branche.

Ich begrüße dann Herrn Michael Leistenschneider. Er ist Mitglied des Vorstands der DATEV eG, einer eingetragenen Genossenschaft. Zur Bedeutung dieser Rechtsform werden wir vielleicht gleich noch etwas hören. Seit 1994 ist er Mitglied des Vorstands, also jemand, der die DATEV sehr gut kennt. Er hat, das muss ich als Betriebswirt einmal kurz erwähnen, bei einem der Urväter der Nachkriegs BWL, nämlich bei Günther Wöhe studiert und sich zum Steuerberater ausbilden lassen. Er ist also sehr stark der BWL und den Steuern verbunden, hat sich aber darüber hinaus immer mit der IT befasst und ist u.a. Mitglied des EDV Ausschusses der Bundessteuerberaterkammer. Er ist ferner Mitglied des Vorstands des Trust Center e.V. von Teletrust und Mitglied des TelekomForum, einer Anwendervereinigung der Deutschen Telekom, kennt also die IT Welt wie auch die sehr sensible Welt der steuerbezogenen Daten sowie der Unternehmen oder Dienstleister, die sich damit befassen.

Dann darf ich Ihnen Herrn Dr. Philipp Räther vorstellen. Er ist bei der bekannten Schweizer Bank UBS in London tätig und dort insbesondere als Jurist für das Datenmanagement zuständig, nicht nur in der juristischen sondern auch in der Managementverantwortung für den Datenbereich. Er hat in verschiedenen Funktionen in internationalen Kanzleien gearbeitet, hat in Freiburg promoviert, seine juristische Ausbildung an verschiedenen Stellen in Deutschland und im Ausland, auch in den Vereinigten Staaten, durchlaufen.

Dann darf ich Herrn Sirtl begrüßen. Er ist Informatiker, bei Microsoft tätig und dort im Schwerpunkt Cloud Computing. Er hat auch ein Buch geschrieben über Cloud Computing und die Möglichkeiten, es mit dem Windows Azur Programm oder der Plattform zu erschließen. Ich darf noch darauf hinweisen, dass er einige Jahre bevor er zu Microsoft kam, bei Accenture tätig war. Er kennt also die IT Service Branche wie auch die Softwarebranche exzellent.

Ich begrüße auch Herrn Dr. Unkel herzlich auf dem Podium. Er ist, wie Sie von heute Vormittag wissen, der Leiter des Bereichs Informationsmanagement bei RWE Power bei der RWE Gruppe in Essen.

Ich denke, dass wir so vorgehen, dass wir zuerst diejenigen unter Ihnen, die sehr kundennah arbeiten bzw. selbst Kunden oder potentielle Kunden von Cloud Anbietern sind, fragen, was sie eigentlich für zwingende Anforderungen haben, um ihr Geschäft möglicherweise einem solchen Cloud Anbieter zu übergeben, denn wir wollen ja versuchen, die Frage unseres Panel zu beantworten: Wann vertrauen Sie Ihrem IT-Versorger? Cloud und Trust in der Kontroverse von Anbietern und Konsumenten. Wir haben uns hier auf dem Panel geeinigt, dass wir den Begriff des Konsumenten weit fassen, dass wir den klassischen, privaten Endkunden, den Endkonsumenten sehen wollen, aber dann auch den geschäftlichen Kunden. Deshalb möchte ich zunächst die drei Vertreter auf dem Panel, die sich täglich mit der Kun-

densicht befassen, ansprechen. Herr Leistenscheider von der DATEV ist selbst ein IT-Service Anbieter, eng verknüpft mit der Steuerberatungsbranche und deren Mandanten draußen, die viele von uns hier wahrscheinlich sind, und um die Daten dieser Mandanten geht es letztlich und um die mögliche Überführung dieser Daten und deren Verarbeitung in der Cloud. Was sind das für Anforderungen, die Sie für unabdingbar halten, Herr Leistenschneider, wenn Sie die Strategie des Cloud Computing verfolgen wollten?

Herr Leistenschneider:
Gestatten Sie mir, nachdem wir heute Morgen dieses Thema verstärkt aus Sicht der Juristen beleuchtet haben, das Ganze einmal aus der Sicht des Steuerberaters zu betrachten. Jeder hier im Saal, der die Presse verfolgt, wird gelesen haben, wie sehr sich der deutsche Fiskus darüber freut, wenn sich Wolken auftun und Steuerquellen aus fernen Ländern sprudeln. Dafür bezahlt man in Berlin mittlerweile Millionenbeträge. In Hinblick auf solche Entwicklungen würde ich aus berufsständischer Sicht Unternehmensdaten generell in zwei Kategorien unterteilen, nämlich einmal in Geschäftsdaten, die für die Berufsausübung benötigt werden, und andere Daten. Letztere sind heute Morgen schon mal als „Mickey-Mouse-Daten" bezeichnet worden. Mit dieser zweiten Gruppe möchte ich mich an dieser Stelle nicht beschäftigen. Bei der ersten Gruppe handelt es sich in der Regel um Mandantendaten, die bezüglich ihrer Weitergabe an Dritte erheblichen rechtlichen Einschränkungen unterliegen. Hier spielt das Verschwiegenheitsgebot als eines der zentralen Berufsgebote, das in gleicher Weise für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte gilt, eine große Rolle. Um dem Risiko eines strafbewährten Geheimnisverrates durch unerlaubte Weitergabe von Mandantendaten zu entgehen, muss der Steuerberater sehr genau hinschauen, wer mit seiner Zustimmung wann welche Mandantendaten einsehen kann. Ein Blindflug in einer Wolke ist für ihn ein unmögliches Unterfangen. Er muss stets wissen und kontrollieren können, was mit den ihm überlassenen Mandantendaten geschieht. Andernfalls riskiert er, sowohl strafrechtlich als auch berufsrechtlich belangt zu werden bis hin zu Geld- und Freiheitsstrafen oder gar einem Berufsverbot.

Mandantendaten selbst lassen sich nochmals unterteilen in steuerrelevante und nicht-steuerrelevante Daten. Dabei sind steuerrelevante Daten nicht nur die Finanzbuchhaltungs- oder Lohndaten. Zu ihnen gehören auch die vielen Emails, die vielen Excel-Sheets und die Word-Dateien, die einen geschäftlichen Bezug haben. Für diese Daten verlangt der Gesetzgeber in § 146 Abgabenordnung, dass sie physisch im Inland aufbewahrt werden. Das ist der bisherige Grundsatz. Nachdem aber dieser Grundsatz nicht mehr den einschlägigen europarechtlichen Vorgaben entsprach, wurde durch das Jahressteuergesetz 2009 aktuell hier eine kleine Kurskorrektur vorgenommen. Danach wurden die Aufbewahrungsmöglichkeiten für steuerrelevante Daten dahin gehend erweitert, dass eine Speicherung nunmehr auch in den anderen EU-Mitgliedsstaaten möglich ist – allerdings mit wesentlich strengeren Auflagen als bei einer Speicherung im Inland. Es muss in jedem Fall gewährleistet sein, dass der

deutsche Fiskus uneingeschränkt auf diese Daten im EU-Ausland zugreifen kann. Sollte diese Voraussetzung oder eine der weiteren gesetzlichen Voraussetzungen wegfallen, so müssen solche steuerrelevanten Daten unverzüglich wieder physisch nach Deutschland zurückgeholt werden. Dazu kann ein Verzögerungsgeld bis zu 250.000 Euro festgesetzt werden.

Zum Schluss möchte ich kurz noch etwas zur DATEV sagen, nachdem die DATEV von Vorrednern schon mehrfach erwähnt worden ist, insbesondere in Hinblick auf das Thema Vertrauen bei Cloud Computing. Die DATEV nimmt hier eher eine Sonderstellung ein, da sie rechtlich gesehen im Verhältnis zu ihren Mitgliedern und deren Mandanten nicht als externes gewerbliches Rechenzentrum gilt. Sie ist berufsrechtlich viel mehr als Berufshelfer bzw. als Erfüllungsgehilfe des steuerberatenden Berufes zu sehen. Sie ist also Teil des Systems, wie das z.B. auch bei Berufskammern oder Berufsgesellschaften der Fall ist. Wenn nun ein Steuerberater die ihm anvertrauten Mandantendaten an ein gewerbliches Rechenzentrum auslagern oder dort weiterverarbeiten lassen möchte, dann muss er dafür explizit die Zustimmung von jedem seiner Mandanten einholen. Ansonsten riskiert er, strafrechtlich belangt zu werden wegen Geheimnisoffenbarung nach § 203 Strafgesetzbuch. Gibt er die Mandantendaten allerdings an einen anderen Berufsangehörigen weiter, dann hat er dieses Risiko nicht, weil der andere Steuerberater den gleichen berufsrechtlichen Gegebenheiten unterliegt wie er selbst.

Bei der DATEV gilt dies in gleicher Weise. Sie ist berufsrechtlich gesehen eine Berufsorganisation wie eine Steuerberatungs- oder Wirtschaftsprüfungsgesellschaft. Die DATEV hat wie jeder Steuerberater ein Zeugnisverweigerungsrecht und es gelten die gleichen Beschlagnahmeregeln. Als Teil des Systems hat sie das Vertrauen der Steuerberater und deren Mandanten, die ihr heute die Buchhaltungs- und Jahresabschlussdaten von über zwei Millionen Unternehmen anvertrauen. Auch, dass man sich schon seit Jahrzehnten berufsständig stets auf Augenhöhe begegnet, fördert und sichert die Vertrauensbildung der Partner untereinander. Das als kurze Einleitung zum Thema.

Prof. Picot:
Vielen Dank. Wir haben gesehen, dass die Anforderungen hinsichtlich Verfügbarkeit, Auffindbarkeit, Schutz, Vertraulichkeit an die steuerlich relevanten Daten sehr hoch sind und dass ein organisatorischer Rahmen gefunden wurde, der auch noch zusätzlich durch die Rechtsform der Genossenschaft gefestigt ist, die der gegenseitigen Förderung dient und daher nicht einen Gewinn zu Lasten der anderen Seite macht, es ist also ein gemeinsamer Kooperationsverbund. Das alles trägt zusammen mit den berufsrechtlichen Regelungen offensichtlich zu einem Vertrauenskontext bei, innerhalb dessen Sie dann – und das wäre meine Frage, die ich noch an Sie stellen wollte –, auch eine private Cloud betreiben. Kann man das so sagen oder ist das nicht der Fall?

Herr Leistenschneider:
Doch, wir bezeichnen das selber als private Cloud. Das ganze ging ja in den 80er Jahren los, wo die DATEV mangels Internet im Endeffekt damals das weltgrößte Corporate Network, also das größte ISDN Netz der Welt aufgebaut hat. Das ist natürlich durch die ganzen Veränderungen in der Kommunikationslandschaft mittlerweile verschwunden. Es gibt nicht mehr diese Kopfstellen, die früher einmal eingerichtet wurden. Heute erreichen Steuerberater und auch ihre Mandanten die DATEV ganz normal über Internet, über VPM Leitungen über das DATEV Net, das wir hier betreiben. Insofern kann man sagen, dass wir eine sehr große Private Cloud betreiben.

Prof. Picot:
Vielen Dank, Herr Leistenschneider. Ich möchte dann als nächsten von der Kundenseite Herrn Dr. Räther aufrufen. Er ist bei der UBS, also im Bankbereich, und da haben wir es auch mit recht sensiblen Themen und Daten zu tun, wie wir alle aus den aktuellen Ereignissen heraus wissen. Mich würde interessieren, was das Anforderungsraster ist, das Sie an eine Cloud bezogene interne und/oder externe Datenverarbeitung richten müssen, richten wollen, damit die Vertrauensbeziehungen zu Ihren Kunden erhalten bleiben?

Dr. Räther:
Sie kennen wahrscheinlich die UBS. Wir sind der weltgrößte Vermögensverwalter, haben aber auch einen großen Investmentbanking-Arm, sind in über 50 Ländern weltweit tätig und unterliegen natürlich dort unterschiedlichsten Regularien. Das Cloud Computing ist für uns sehr interessant, da wir auch unter einem großen Kostendruck stehen. Unsere IT Systeme verschlingen sehr viel Geld. Gleichzeitig müssen wir aber mit sehr vielen Regeln compliant sein. Das Hauptproblem sind territoriale Probleme beim Cloud Computing. Sie wissen alle, viele Länder haben ein Bankgeheimnis. Das der Schweiz, zum Beispiel, werden Sie kennen. In Europa sind es aber noch etliche andere Jurisdiktionen und weltweit (zum Beispiel in Korea, China, Singapur, Mexiko) kommen Sie bald auf über ein Dutzend Jurisdiktionen. Was diese Regeln alle gemein haben ist, dass, wenn Sie eine Bankbeziehung haben, diese Information im Land bleiben muss. Das heißt auch, dass diese Information nicht einmal verschlüsselt auf irgendeinem anderen Server im Drittland stehen darf. Das ist natürlich nicht kompatibel mit einer Cloud Computing Lösung, wo man flexible Speicher-Länder hat. Wenn wir so etwas machen würden, wäre dies eine Anforderung, die Speicherländer festzuschreiben.

Einige Länder gehen sogar noch weiter und sagen, dass nicht nur das Land die Grenze ist, sondern sie geben vor, dass Kundendaten von Privatkunden und Investmentkunden getrennt gespeichert werden müssen. Das sind die sogenannten APAC Firewall-Regeln.

Mit dem heute Morgen gesagten Schlagwort beim Cloud Computing sind ‚die Daten irgendwo', könnten wir sicher nicht leben. Aber auch wenn Sie kein Bankgeheimnis

haben, also wenn viele Länder das durchaus zulassen, dass die Daten im Ausland gespeichert werden, ist es für uns ein ziemliches Risikopotenzial aus Sicht der Kunden, weil wenn die Daten einmal in den USA sind, es große Begehrlichkeiten der Steuerbehörden gibt einmal zu schauen, was denn da die Kunden im Ausland eigentlich machen. Aus der Sicht unserer Kunden und unserer Reputation wollen wir solche Szenarien eher vermeiden. Es gibt also territoriale Probleme in den Griff zu kriegen.

Ein weiteres Problem klang heute Morgen schon oft an. Wir haben natürlich nicht nur institutionelle Kunden sondern auch viele Individuen. Da ist das Datenschutzgesetz anwendbar und, wie heute auch schon oft gesagt worden ist, gemäß der EU Datenschutz-Richtlinie und des BDSG und anderer nationaler Gesetze müssen personenbezogene Daten im EU-Raum bleiben. Wir haben aber auch schon Outsourcing-Vorhaben, wo die Daten dann in Indien sind, aber nicht in einer Cloud. Da bietet sich an, Verträge aufgrund der Vorgaben der EU Kommission zur Auftragsverarbeitung zu schließen, wonach sich der Provider einfach freiwillig zu einem höheren Datenschutzniveau verpflichtet, der dem in der EU, z.B. in UK, Deutschland oder Schweiz, entspricht. Aus Sicht des Datenschutzes der Individuen sehen wir durchaus Lösungsmöglichkeiten.

Ein weiterer kritischer Punkt ist die IT Sicherheit: Key ist der Schutz von Bankdaten. Sie haben wahrscheinlich alle von dem „Danger"-Fall gehört, eine Microsoft Tochter, die letztes Jahr einiges an Telekommunikationskundendaten verloren hat, die nicht wiederbringbar waren. So etwas wäre natürlich für eine Bank ein Fiasko. IT-Sicherheit hat bei uns oberste Priorität.

Der vorletzte Punkt wurde heute auch schon mehrfach genannt. Das sind natürlich die Aufsichtsbehörden. Wir müssen als Finanzunternehmen jedes materielle Outsourcing den Aufsichtsbehörden melden; in Deutschland der BAFin, in den UK der FSA. Meines Wissens ist noch nicht getestet, inwiefern die Aufsichtsbehörden mit dem Cloud Computing d'accord sind. Das hängt wohl sehr von der Ausgestaltung ab und insbesondere ob die territorialen Probleme in den Griff zu kriegen sind.

Der letzte Punkt ist vielleicht noch ganz interessant. Er ist heute noch nicht genannt worden und kommt hauptsächlich aus dem US Bereich, und zwar aus dem Prozessrecht. Die SEC und verschiedene andere Aufsichtsbehörden erfordern, dass sie den Beweiswert ihrer Daten nicht verändern. Die müssen 'WORM compliant' sein. Und WORM heißt „Write Once Read Many", d.h. sie müssen in einer bestimmten Art und Weise gespeichert werden, damit gewährleistet ist, dass sie diese Daten nicht verändert haben. Diese Beweiskraft spielt dann natürlich in E-Discovery Verfahren, bei Prozessen und aufsichtsrechtlichen Verfahren eine große Rolle. Die Anbieter eines Cloud Computings müssen auch gewährleisten, dass sie nach diesen Standards die Daten speichern. Ich weiß nicht, ob das technisch beim Cloud Computing geht und wie flexibel die Server dann noch wären.

Fazit: Cloud Computing ist durchaus interessant für uns, es hat aber noch viele Fragezeichen und zu lösende Probleme.

Prof. Picot:
Vielen Dank, Herr Dr. Räther. Wenn man hört, welche Restriktionen existieren und welche Vorschriften zu beachten sind, auch für die Eigeninteressen einer Bank, damit nichts passiert, möchte ich Ihnen eine kleine Anschlussfrage stellen: Reicht Ihre Phantasie aus, dass jemand in Ihrem Hoheitsbereich irgendwie eine CD mit Kundendaten zieht und die dann an eine andere Regierung weitergibt?

Dr. Räther:
Ja, das ist ja durchaus schon passiert bei anderen Banken, wie wir alle gehört haben. Unsere IT-Sicherheit sollte jedoch garantieren, dass so etwas bei uns nicht passiert.

Prof. Picot:
Unabhängig von den beteiligten Banken ist es einfach interessant, auch von Fachleuten zu hören, wo und wie Sie glauben, dass solche doch sehr hoch gesicherten, hoch durchdachten und regeldurchdrungenen Systeme doch löchrig werden können. Denn das ist doch das, was Sie gerade vermeiden wollen. Ich denke mir, dass intern bei Ihnen viel darüber geredet wird, wie man das vermeiden kann, extern wahrscheinlich weniger.

Ich möchte dann Herrn Dr. Unkel fragen, was er uns aus seiner Kundensicht sagen kann. Sie haben das heute früh schon aus der IT Managementsicht schön aufbereitet. Aber wenn Sie sich jetzt den Hut einmal als Geschäftskunde aufsetzen, aber auch als Vertreter Ihrer Endkunden, die Sie ja auch haben und von denen Sie leben, und deren Daten bei den Providern zunehmen – wir haben es heute früh nur kurz anreißen können. Kundendaten spielen in dem energiewirtschaftlichen System eine wichtige und in Zukunft noch stärkere Rolle. Was muss geschehen, damit diese hohen Anforderungen an die Massendatenverarbeitung, die sehr effizient sein soll und deshalb auch die Cloud benötigt, dorthin transferiert werden kann, ohne dass Ihre Kunden Schaden nehmen?

Dr. Unkel:

Ja, ich hatte heute Morgen in meinem Vortrag schon die Anforderungen von RWE Power ausgeführt. Deswegen kann ich mich hier kürzer fassen. Wir sehen Unklarheiten und auch Risiken, die heute auch in den verschiedenen Vorträgen zum Ausdruck gekommen sind. Die Energiewirtschaft gehört zu den kritischen Infrastrukturen, die soeben auch im Vortrag von Herrn Schallbruch vom Bundesministerium des Inneren erwähnt wurden. Unsere Kunden müssen einfach erwarten können, dass wir verantwortungsvoll mit der Versorgungssicherheit und konkret auch mit ihren Kundendaten umgehen. Das grenzt die Möglichkeiten der Nutzung von Cloud Computing ein. Ich würde es aber nicht grundsätzlich als unmöglich ansehen. Ich hatte heute Morgen schon darauf hingewiesen, dass sich insbesondere bei echten IT Commodities mit Cloud Computing vielleicht neue Standards am Markt etablieren können. In diesem Bereich geht es also nicht um kritische Daten, sondern um Standardfunktionen, die auch für uns nutzbringend sein können.

Ich sehe weiterhin eine Chance in dem Architekturprinzip, das mit Cloud verbunden ist, im Sinne der Ausprägung einer Private Cloud. Daraus werden weitere Erfahrungen gewonnen zum Umgang mit Cloud Computing. Parallel dazu werden wir verfolgen, wie sich der Cloud Computing Markt entwickelt. Wird es wirklich eine weitere Marktverbreitung geben, so dass der für uns wichtige Nachhaltigkeitsaspekt zum Tragen kommt? Die Anbieter von Cloud Computing werden sicher beobachten, wie die Endbenutzer die Vorzüge des Architekturprinzips annehmen. Werden die Vorzüge darin bestehen, dass die Benutzer eigentlich keinen FAT Client PC mehr brauchen, weil sie die Funktionalität aus der Cloud beziehen? Werden sie weiterhin FAT Client PC kaufen? Die Masse der heute verkauften PC ist nach wie vor vom Typ FAT Client. Hat die Cloud Industrie dann nicht einen schweren Stand bei dieser weit verbreiteten FAT Client Basis? Ich denke hier an das Beispiel der Magnetschwebebahn, die sich bei uns bisher auch deshalb nicht verbreiten konnte, weil es bereits eine installierte, schienengebundene Bahn gab.

Die Marktverbreitung ist für uns wesentlich, wir werden sie beobachten. Daneben werden wir weitere Erkenntnisse und eigene Erfahrungen mit Cloud Computing sammeln.

Prof. Picot:
Vielen Dank. Das ist ein interessanter Punkt mit der installierten Basis, die eben eine andere Funktionalität aufweist und möglicherweise auch die Abhängigkeitsprobleme reflektiert, die zum Teil bei dem Cloud Computing gesehen werden. Ich spreche jetzt vom einfachen Endkunden – wenn der einen FAT Client hat und alles Mögliche immer runterlädt, dann hat er zumindest die Illusion, dass er noch unabhängig von der Vernetzung sei und für sich die Datenverarbeitung und -analyse vornehmen könnte, wenn mal das Netz nicht verfügbar wäre. Das ist ein interessanter Punkt, den wir vielleicht im Folgenden noch aufgreifen.

Bis hierher haben wir sehr interessante und zum Teil extrem hohe Anforderungen gehört, die sich an das Cloud Computing richten aus der Sicht von unterschiedlichen Anwendern, Anbietern und Verarbeitern kritischer Daten. Wenn ich mir vorstelle, ich wäre ein Anbieter von Cloud Computing, muss man dann nicht die Segel streichen und sagen: Es tut mir leid, das war es, ich schaffe es nie, diese Anforderungen alle zu erfüllen? Oder gibt es realistische Perspektiven bzw. muss sich das Cloud Computing auf solche Verarbeitungsbedarfe konzentrieren, bei denen das Anforderungsniveau eben nicht so hoch ist? Da würde ich gern die Kollegen aus dem Bereich der Anbietergruppe bitten, sich dazu zu äußern. Vielleicht gehen wir auch hier wieder in der Reihenfolge vor, wie sie sich aus dem Programm ergibt. Ich darf als erstes Herrn Auerbach bitten, aus der Sicht von T-Systems uns seine Perspektive zu geben.

Herr Auerbach:
Vielleicht ganz kurz ein Wort zu T-Systems. T-Systems ist die Großkundensparte der Deutschen Telekom. Wir kümmern uns um die 400 größten Kunden und liefern Rechenzentrumsdienstleistungen, Enduser Computing, Netzwerkleistungen, aber auch Systemintegrationsleistungen für die Geschäftskunden der Telekom. Dazu gehören zum Beispiel BMW, Daimler und VW. Beim Cloud Computing unterscheiden wir prinzipiell das Geschäft mit Endkunden vom Geschäft mit Unternehmenskunden. Die Anforderungen sind einfach grundsätzlich anders. Endkunden finden ihre Plattform bei T-Online. Jeder kennt den Immobilienscout oder den Autoscout. Das ist eine klassische Cloud Anwendung. Sie geben die Beschreibung ihrer Immobilie in ihrem PC ein, speichern dies irgendwo hin und wundern sich am kommenden Tag über die zahlreichen Anrufe und Mails von Leuten, die ihr Haus kaufen wollen. Oder Sie laden im klassischen Printservice Bilder hoch und am nächsten Tag steht der Briefträger mit Ihren Abzügen vor der Tür. Dies sind für mich klassische Cloud Anwendungen. Sie laden Ihre Bilder irgendwohin in die virtuelle Welt, wissen nicht, was dann weiter passiert und dann klingelt der Briefträger an Ihrer Tür und präsentiert ihnen das Endergebnis.

Diese Cloud-Computing-Welle rollt und nimmt immer stärker Fahrt auf. Ich fand es sehr interessant auf dieser Tagung zu sehen, wie jetzt viele Soziologen, Rechtsanwälte, Datenschützer versuchen zu beschreiben, was Technik und IT bereits real geschaffen haben. Eine Entwicklung, die nicht mehr aufgehalten werden kann.

Ein prinzipiell anderes Vorgehen sehen wir bei den Businesskunden. Im privaten Haushalt haben wir momentan relativ flache Datenstrukturen. Es geht um ein Bild oder ein Video, das hochgeladen wird. Etwas komplexer wird es bei einer E-Mail. Selbst wenn ich Informationen nehme wie die Videoüberwachung am Freiburger Bahnhof oder Kreditkartengeschäfte, die getätigt werden: Das massenhafte Verknüpfen von Daten, um sie personenbezogen auszuwerten, gehört aktuell immer noch in Teilen in den Bereich von Science Fiction.

Anders ist es im Businessbereich. Dort sind die Datenstrukturen extrem komplex. Ein relativ einfacher Datensatz wie eine Adresse ist schon sehr stark relational. Dies bedeutet, eine Adresse wird heute benutzt sowohl vom Marketing, vom Vertrieb, von der Logistik, von der Faktura und schlussendlich vom Inkasso. Es muss genau geregelt werden, wer diese simple Adresse eingeben darf, wer Veränderungen vornehmen darf und wer der Eigentümer dieser Adresse ist. So sind die Security-Mechanismen innerhalb einer einzelnen Firma ausserordentlich komplex, die den Umgang mit diesen Daten regeln. Geregelt ist der Umgang mit Applikationen und Administrationsrechten, teilweise sogar runter bis auf die Firewall und Systemeinstellungen.

Jetzt treffen diese beiden Welten aufeinander: Ich möchte die hochskalierten, hochautomatisierten, industrialisierten, selbstadministrierten, standardisierten Cloud-Welten mit dieser komplexen Businesswelt verbinden – eine Herausforderung. Denn es zeigt sich meiner Meinung nach, dass es nur bedingt möglich ist, die Komplexität

des Business in die heute bestehenden Clouds zu übertragen. Sichere Business Prozesse können teilweise überhaupt nicht abgebildet werden. Bekomme ich es doch hin, geht sehr oft die Effektivität verloren. Ebenfalls gibt es Probleme, meine Daten revisionssicher aus der Cloud zurück zu laden.

Wir von T-Systems gehen einen eigenen Weg. Wir denken, dass es eine hohe Korrelanz gibt zwischen den öffentlichen Clouds, in der die Privatdaten liegen und den Business Clouds, in denen die Geschäftskunden arbeiten. So sind wir dabei, die Plattformen, die wir für unsere Geschäftskunden betreuen, nach den gleichen Mechanismen, den gleichen Methoden und Verfahren der öffentlichen Clouds zu betreiben, aber darauf gleichzeitig die Komplexität der Geschäftskunden abzubilden. Ich denke, in Zukunft wird es sogar eine richtige Koexistenz geben. Momentan laufen einige Pilotprojekte mit Kunden, in denen die ganz einfache Mailbox bei einer Microsoft oder einer Google durchaus in der Public Cloud liegt und die sicherheitsrelevanten Businessstrukturen in einem komplexen Sharepoint bei uns in der geschützten und abgeschotteten Cloud. So arbeiten wir gerade daran sicherzustellen, dass sich beide Welten unterhalten können. Ich bin fest davon überzeugt, dass die Cloud im Business nicht mehr aufzuhalten ist. Die meisten unserer Neukunden gehen davon aus, dass wir bis zu 80% ihrer Anwendungen in die Cloud Plattform legen werden. Wir sind aktuell mit Hochdruck dabei, täglich und an jedem Wochenende größere Mengen von Servern und Applikationen umzustellen. Das funktioniert, weil wir es schaffen, die bewährten Security Mechanismen aus den klassischen Umgebungen ebenfalls auf die neuen Plattformen anzuwenden, die wir entsprechend skalieren. Auch alle aktuellen kritischen Fragen, wo liegen die Daten und wer hat Zugriff, können wir heute bereits beantworten und zur Zufriedenheit unserer Kunden abbilden.

Ich denke, die öffentlichen Clouds werden immer schneller. Die Businessanwendungen werden diese Technologie immer stärker nutzen. Und die aus heutiger Sicht bestehenden Hindernisse, werden sukzessive abgearbeitet.

Prof. Picot:
Vielen Dank, Herr Auerbach. Wir haben also gesehen, private und öffentliche Cloud nebeneinander, ähnlich leistungsfähig in der Perspektive. Herr Dueck, Sie haben mit Ihrem Haus IBM seit vielen Jahren schon den Slogan „on Demand“, dass man also alles Mögliche on Demand beziehen können soll aus dem großen Panoptikum der IT-Welt. Wie ist Ihr Erfahrungsstand auch vor dem Hintergrund der Kundenanforderungen? Wo sind da die Grenzen des „on Demand“ bzw. wo sind unausgeschöpfte Möglichkeiten, um diesen Anforderungen gerecht zu werden?

Prof. Dueck:
Ich sehe das etwas betriebswirtschaftlicher. Also nicht so sehr von der Security her. Das regelt sich hinterher. Vielleicht ist das eine typische Einstellung eines „Techies“, Techies regeln das später. Ich gebe Ihnen einmal ein paar Beispiele für den Wandel von Infrastrukturen. Als die Waschmaschine aufkam – kennen Sie das

noch? Da hieß es: „Die wäscht nicht weiß." Darin spiegeln sich Ängste von Hausfrauen wider, die sich für zwei, drei Jahrzehnte in meiner Jugend in der Werbung festgebissen haben. „Persil wäscht weißer und Ariel wäscht noch weißer." Jetzt interessiert es keinen mehr, jetzt wäscht es einfach weiß. Das Wichtigste aber war: Die Wäsche musste umgestellt, nämlich normiert werden. Die ganze Textilindustrie produziert heute Wäsche, die bei 30, 60 oder 90 Grad gewaschen wird. Es gibt kaum etwas anderes. Es gibt keine 71 Grad zwischendurch. Alles muss sich dem Standard anpassen. Nach der Waschmaschine haben Sie sich eine Geschirrspülmaschine gekauft. Da sind Ihre Kristallgläser milchig rausgekommen. Und heute produziert die ganze Industrie dafür taugliche Standards, nämlich Gläser, die geschirrspülgeeignet sind. Dieser Punkt interessiert heute auch keinen mehr, weil das für uns heute selbstverständlich so ist. Das ist erledigt und aus unserem Sinn heraus. Die ganze Umstellung der Produkte dauert aber 10 Jahre und mehr! Sie haben sich danach einen Trockner gekauft. Der lässt alles einlaufen, usw. Ich könnte jetzt stundenlang erzählen. Die Probleme, worüber Sie sich jeden Tag aufgeregt haben und Bedenken ohne Ende äußerten, wurden nicht in der Waschmaschine gelöst, sondern in der Wäsche. Alles, die Maschine und die Wäsche, mussten aufeinander zugehen. Wäsche und Geschirr wurden normiert. Genauso wie in diesen historischen Fällen sehe ich den Fall auch bei Cloud Computing. Die heutigen Anwendungen passen in aller Regel für eine Cloud ebenso nicht wie die erste Wäsche für den Trockner. Anwendungen müssen so standardisiert werden, dass sie „cloudfähig" sind. Danach sparen sie mit Cloudanwendungen Geld und haben ein bequemeres Leben.

Die ersten kommerziellen Clouds üben auch schon einen enormen Preisdruck aus. Ressourcen aus einfachen Clouds wie die EC2 von Amazon sind sehr billig. Sie können ja einmal versuchen, Ihren Laptop zu den Amazon-Konditionen gewinnbringend zu vermieten. Wenn Sie durchrechnen, dass Sie für ein Gigabyte Speicher im Monat nur 6 Cent bekommen, verstehen Sie, wie kostengünstig standardisierte Ressourcen im Netz sind.

Das wird beim Diskutieren über Clouds oft vergessen. Die meisten streiten noch, was alles bei Cloudlösungen von der Funktionalität her nicht gut ist, aber irgendwann sieht man die geringen Kosten! Die werden hier gar nicht besprochen, sind aber der größte Pain Point. Die potentiellen Cloudkunden leiden unter Kostendruck und müssen ihre IT jedes Jahr, 10, 20% billiger machen. Und das geht ja mit diesen industrialisierten Lösungen! Und deswegen kommt aus betriebswirtschaftlichem Druck ein Standardisierungsdruck in die IT. Ich will es einmal so nennen – dass Wort habe ich dafür erfunden: Die IT wird einem Reengineering unterzogen werden, das ich mit „IT-Resource-Planning" bezeichnen möchte, analog zu „Enterprise Resource Planning" oder „SAP R/3" in der klassischen Produktion.

Wir fangen jetzt an, über Service Managementschichten (das geschieht etwa über IBM Tivoli) so eine Art „SAP R/3" in der IT einzuführen. Wie in der Automobilindustrie alle Prozesse durch ERP-Systeme standardisiert wurden, so können wir heute mit IT Servicemanagement alle Prozesse in der IT so umstrukturieren und effizienter machen, dass hinterher alles vielleicht mit einem Drittel der Ressourcen her-

stellbar ist. Am Ende der Ideenkette steht die völlige Industrialisierung der IT durch „Cloud Computing Konzepte“.

Eine solche Entwicklung ist absehbar, wenn sie auch heute noch auf Unglauben stößt. Hätten Sie denn zu der Zeit, als Toyota Mitte der 80er Jahre die zweite Revolution in der Automobilindustrie einleitete, die heutigen Produktionsdaten für möglich gehalten? Alles wird mit einem Bruchteil der Ressourcen produziert, die Qualität ist gestiegen, die Autos haben heute kaum noch Pannen, sie kommen in Stunden statt in Tagen vom Band, bei ganz wenigen verbliebenen Mitarbeitern. Auch heute werden noch dauernd Leute in der Autoproduktion entlassen, und es kommen immer noch mehr Autos raus. Wundert Sie das nicht?

Dieser Prozess der Industrialisierung der IT schreitet jetzt ebenso rasch voran, und Cloud Computing ist eine Hauptidee dieser Entwicklung. Das funktioniert alles jetzt nicht gleich sofort. Die komplexesten Lösungen einer Großbank sind absolut nicht einfach „cloudifizierbar“ und werden auch sicher nicht in Public Clouds auftauchen. Man fängt mit den Anwendungen an, die leicht cloudifizierbar sind. Das sind etwa Maillösungen oder virtuelle Festplatten für Private! IBM hat heute schon das Mailangebot LotusLive mit über 10 Millionen Seats verkauft. Der größte Vertrag mit Panasonic umfasste neulich über 300.000 Nutzer.

Ich möchte auch zur Kenntnis geben, dass sich das Denken über Cloudlösungen rasch zugunsten von Clouds ändert. Auf einer Konferenz wie der jetzigen, wenn sie vor einem Jahr stattgefunden hätte, würde hier wahrscheinlich abwehrend gejammert, etwa so: „Die Mail des Unternehmens werde ich **nie** auf eine Cloud geben, weil das alles so geheim ist, was ich da in den Computern habe“. Was ist da so geheim? Meine Assistentin liest ja schon alles mit, auch die Fanpost von Lesern meiner Bücher. Die Furcht, dass da wichtige Geheimnisse im Netz ausspioniert werden, geht irgendwie an der Wirklichkeit vorbei. Der Widerstand gegen das Netz schwindet und wir werden die Mail bald überwiegend in Netz haben.

Google und IBM nehmen für den Mailservice heute so etwa 30 Euro im Jahr. Angesichts dieser Marktpreise müssen sich IT-Dienstleister fragen, wie hoch ihre internen Herstellkosten eigentlich sind. Sind sie vergleichbar niedrig? Nicht nur bei Maillösungen werden Marktpreise entstehen. Bald werden an allen wesentlichen IT-Services Preisetiketten kleben.

Und Sie werden als CIO mehr und mehr gefragt werden, wie viel alles bei Ihnen kostet. Wissen Sie das überhaupt? Können Sie das aus Ihrer Kostenrechnung überhaupt ersehen? Oder müssen Sie schamrot werden, weil Sie zu teuer produzieren?

Sie werden sich beim Vergleich mit Preisen der Public Clouds winden und zu Recht auf bessere interne Netze und größere Ausfallsicherheit verweisen können, aber die Preise bleiben einfach im Raum stehen und über Druck auf die IT aus. Der CFO des Unternehmens wird nachfragen. Dieser Druck aus der Finanzecke setzt die Industrialisierung der IT in Gang. Die Bewegung ist angelaufen und nicht mehr aufzuhalten. Das Sparen treibt viel stärker als die Entwicklung der Technologie. Wir

stehen vor einem ganz normalen Industrialisierungsvorgang irgendeiner Industrie. Mit Mail Services startet alles, danach werden Testumgebungen, dann Entwicklungsumgebungen in die Cloud wandern…

Wie wird es nach der Cloud weitergehen? Dazu können Sie ja jetzt gleich die Strategie von Google erklären. Auf dem Consumer Level gibt es schon Google Apps. Die Vorstellung ist, dass man sich gar nicht mehr mit IT als solcher befasst und man gar keine Computer, keine IT mehr mietet, sondern einfach nur den Service erhält. So wie bei Google Apps Privatkunden das Navi als Service mieten, werden Unternehmenskunden zum Beispiel die ganze Kundendatenverwaltung oder die Gehaltsabrechnung aus dem Netz wie eine App beziehen und pro Leistung oder pro Kunde oder pro Angestellten bezahlen. Sie nehmen einfach nur den Service und der kommt von irgendwoher. Für die volle Entwicklung in dieser Richtung fehlt uns jetzt im Augenblick noch die Phantasie. Ich könnte mir vorstellen, dass auf dieser Idee später ganz neue Industrien möglich werden, die es heute noch gar nicht gibt. Ein Beispiel ist von Gunter Müller genannt worden: Eine ganze Firma kann sofort ohne eine eigene IT hochfahren. Solche Businessmodelle werden später in immer größerem Umfang möglich sein.

Prof. Picot:
Vielen Dank. Sicherlich ist ein wichtiger Punkt, der heute noch wenig zur Sprache kam, dass Geschäftsmodelle kippen, sich aber auch neu etablieren können. Das ist natürlich auch ein laufender Prozess des dynamischen Wettbewerbs, in dem im Zeitablauf bestimmte Dinge untergehen und andere sich neu durchsetzen. Das wäre auch der Anknüpfungspunkt für meine Frage an Herrn Gutzeit. Eben sagte schon Herr Dueck, dass Sie mehr die Konsumentenseite betreuen würden und er oder andere dann vielleicht die Geschäftskundenseite. Ich würde an Sie die Frage stellen, ob das eigentlich so stimmt, denn wenn ich mir in Erinnerung rufe, dass ich letzte Woche mit einem Startup Team bei uns an der Uni ein Gespräch hatte, das die Google Cloud nutzt für eine riesige Datensammlung und Datenverwaltung für einen speziellen Service, den dieses Team für den Wissenschaftsbereich jetzt entwickelt. Da werden Daten in einem Volumen für sehr wenig Geld gehostet und verwaltet. Dann scheint es doch so zu sein, dass Unternehmen mit anspruchsvollen Daten basierten Geschäftsmodellen in diese „Consumer Cloud“ gehen können. Oder gibt es doch solche Restriktionen, dass zum Beispiel die Anforderungen, die wir gehört haben aus den Banken und dem Steuerbereich, von einer solchen Consumer Cloud nie erfüllt werden können?

Herr Gutzeit:
Wie so oft, wenn Google auf einer Bühne präsent ist, wird Kritik geübt. Den Wahrheitsgehalt dieser Kritik zu überprüfen und ausführlich zu diskutieren, sprengt den Rahmen dieser Diskussionsrunde. Gern lade ich aber Herrn Prof. Dr. Müller zu uns ein, um sich unsere Produkte und Lösungen einmal näher anzusehen und sich ein Bild zu machen.

Um auf Ihre Frage zurückzukommen: Ich bin als Head of Google Enterprise DACH & Nordics verantwortlich für den Geschäftskundenbereich in Zentraleuropa. Wir bei Google Enterprise bieten spezielle Angebote für Geschäftskunden an. Darunter fällt insbesondere unsere Google Apps Premier Edition, die vor mittlerweile sechs Jahren rund um das Thema E-Mail entwickelt wurde und kontinuierlich weiterentwickelt wird. Das Ganze hat als ein 20%-Projekt eines unserer Ingenieure begonnen. Er war einfach nicht zufrieden mit der Suchfunktionalität seines E-Mail-Clients und hat dann ein eigenes Produkt entwickelt. In diesen sechs Jahren haben wir eine Vielzahl von Entwicklungsschritten vorgenommen und bieten mit der Google Apps Premier Edition ein innovatives, fortschrittliches und kostengünstiges Messaging- und Kollaborationstool für Unternehmen an. Womit ich auf den zweiten großen Punkt hier in der Runde zu sprechen komme: Wir haben etwas über Kosten gehört, insbesondere über Kosteneinsparung. Das ist einer der ganz wichtigen Faktoren speziell in der wirtschaftlichen Situation, mit der wir im letzten Jahr konfrontiert wurden. Ich sage nur „Weltwirtschaftsrezession" und der damit für viele Unternehmen einhergehende Zwang zu Kostensenkungen.

Ein weiterer für uns bei Google immens wichtiger Aspekt ist Innovation. Speziell um das ganze Thema Messaging und Collaboration, grob gesagt um das Thema E-Mail herum, zeichnet sich die Google Apps Premier Edition durch eine hohe Innovationsfähigkeit aus. Für Sie als Geschäftskunde hat das beispielsweise den Vorteil, dass Sie sich nicht permanent darum kümmern müssen, Ihre eigene In-House-Lösung in irgendeiner Art und Weise zu aktualisieren, aufzurüsten, nachzurüsten, nachzupatchen, aufzupatchen, etc. Sie haben stattdessen sofort die Möglichkeit – über ein kleines Häkchen in den Administrationseinstellungen – weitere Funktionalitäten, die unsere cloudbasierte Lösung bietet, zu nutzen oder darauf zu verzichten. Allein im letzten Jahr haben wir unserer Google Apps Premier Edition über 58 neue Leistungsmerkmale hinzugefügt.

Zum Beispiel haben Sie als Unternehmer die Möglichkeit, mit Google Video einen Online-Video-Kanal innerhalb Ihrer Firma zu nutzen, ohne dass Sie einen Pfennig dazu bezahlen müssen. So können Sie beispielsweise Ihre Schulungsvideos oder Ansprachen des CEOs oder des Abteilungsleiters ganz einfach in die Cloud hineinstellen und jedem Ihrer Mitarbeiter verfügbar machen – von überall, jederzeit und auf jedem internetfähigen Gerät. Somit komme ich zu den mobilen Geräten, die schlussendlich unsere Angebotspalette logisch abrunden. In dieser Gesprächsrunde haben wir etwas über FAT Clients gehört. Ich persönlich sehe den Trend eigentlich eher in die entgegengesetzte Richtung. Wenn wir uns die Absatzzahlen für Netbooks anschauen, Apple's Vorstellung des iPad und unser Betriebssystem Chrome OS, sind das alles Produkte im weitesten Sinne, die Minimalanforderungen an Computerleistungen stellen, weil der Fokus auf Cloud Computing liegt. FAT Clients sind dann einfach nicht mehr notwendig, wenn man alles in die Wolke verlagern möchte.

Gern möchte ich auch noch die rechtlichen Aspekte ansprechen. Google Enterprise bietet Unternehmenslösungen an, und sicherlich ist heute nicht jeder Wirtschafts-

zweig prädestiniert dafür, sofort mit Mann und Maus in die Wolke zu gehen. Der Gesetzgeber schreibt gewisse Regularien vor, die – wenn man sich speziell die Entwicklung der Cloud Computing-Thematik genau anschaut – möglicherweise nicht mehr ganz zeitgemäß sind und die man hinterfragen und überdenken kann. Wir sind gern bereit, auch hier unsere technologische Erfahrung mit einzubringen.

Ein weiterer großer Aspekt ist Produktivität. Ich bin überzeugt davon, dass Cloud Computing-Lösungen die Unternehmensproduktivität steigern. Denken Sie an das Thema Echtzeitkollaboration. Verfügt ein Unternehmen über eine Lösung, mit der die Mitarbeiter gleichzeitig, egal von welchem Ort, in Echtzeit gemeinsam an einem Dokument, einer Präsentation oder einer Tabellenkalkulation arbeiten können, ohne dass sie Versionszyklen nachvollziehen oder Dokumentversionen per Email hin- und herschicken müssen, profitiert es von realer Echtzeitkollaboration und spart Zeit und Geld.

Ein letzter Aspekt, den ich gern bezüglich der rechtlichen Thematik nachtragen würde, ist: Ich denke, Google hat im Laufe der Jahre eine der größten Cloud aufgebaut, die es überhaupt gibt und hat einen Innovationsvorsprung von 1,5 bis 2 Jahren. Wir sind heute einer der größten Serverhersteller der Welt, aber wir verkaufen keine Server, sondern benutzen sie ausschließlich für unseren Eigenbedarf, um unsere Datenzentren aufzubauen. Wenn Sie mich jetzt fragen möchten, wo unsere Datenzentren sind, ich kann es Ihnen nicht sagen. Ich selber als Google Mitarbeiter weiß nicht, wo unsere Serverfarmen sind. Hier fängt für Google schon das Thema Datensicherheit an. Wir machen nicht öffentlich, dass unsere Datenzentren in der Hanauer Landstraße oder an sonstigen Peering Points stehen. So vermeiden wir mögliche Angriffe von Hackern, wie beispielsweise den Angriff auf die Rechenzentren eines Mobilfunkanbieters in London vor zwei Jahren. Bei jeder unserer Google-Anwendungen steht Sicherheit im Mittelpunkt, von Beginn an. Dabei hat der Schutz der Daten und des geistigen Eigentums unserer Kunden die höchste Priorität. All unsere Produkte werden unter dieser Maxime entwickelt und sind zudem hoch skalierbar. Und wir können unseren Geschäftskunden diese Sicherheitsstandards auch durch entsprechende Service Level Agreements garantieren.

Ich lade jeden herzlich dazu ein: Googeln Sie mich und mein Team. Gern können wir die Gespräche im Einzelnen führen, um die rechtlichen Themen zu beleuchten.

Prof. Picot:
Vielen Dank. Wir sehen, dass aus dieser Perspektive doch die große Google Cloud, aus der Sicht von Ihren Geschäftserwartungen her, für den privaten wie auch für den geschäftlichen Kunden in gleicher Weise zur Verfügung steht und auch ähnliche Funktionalitäten anbietet.

Ich möchte nun Herrn Sirtl ums Wort bitten. Sie haben etwas warten müssen aber auch überlegen können, was für Sie noch an Goodies übrig bleibt. Ich möchte aber darauf hinweisen, dass Microsoft seit einiger Zeit dieses Cloud Computing als Produkt mit der Plattform Azur anbietet und insofern schon recht früh in einer standar-

disierten oder industrialisierten Art und Weise am Markt ist. Sie können auch über Erfahrungen, aber vielleicht auch über Grenzen berichten, denn wir wissen, dass es nicht etwas gibt, was nur Vorteile hat. Was können Sie uns sagen?

Herr Sirtl:
Microsoft ist seit einigen Jahren im Betrieb großer Rechenzentren unterwegs, auf denen wir unsere eigenen Webseiten betreiben, microsoft.com, msdn.com usw. Von daher haben wir schon jahrelang Expertise, die wir jetzt über unsere Online Services bzw. unsere Azur Plattform auch an die Kunden weitergeben wollen. Der Wunsch ist von den Kunden ganz klar da, von den Kosteneinsparungen, von den Effizienzsteigerungsmaßnahmen, die wir durchgeführt haben, auch zu profitieren. Ich möchte ganz kurz auf Ihre Eingangsfrage zu Beginn des Panels antworten, ob jetzt der große Pessimismus angesagt ist. Wir haben heute im Laufe des Tages viel über Beschränkungen, rechtliche Fragestellungen, die noch geklärt werden müssen, gesprochen. Da bin ich natürlich ein ganz großer Verfechter des Optimismus. Ich bin davon überzeugt, dass vieles von dem, was wir hier so an Produkten, an Plattformen sehen, noch in einem frühen Stadium ist, aber die nächsten Jahre werden zeigen, dass hier durchaus Vertrauen am wachsen ist. Auch wie es Herr Prof. Dueck so schön ausformuliert hat mit dem Waschmaschinenbeispiel, denke ich, dass so etwas in der IT viele Jahre braucht. Wer hätte gedacht, dass eine SAP maßgebliche Teile ihrer Software in Indien fertigen lässt. Oder dass mit Salesforce ein Unternehmen da ist, das sehr erfolgreich CRM Software in der Cloud betreibt. Das sind Beispiele dafür, wo es den Anbietern gelungen ist, über die Jahre hinweg Vertrauen zu schaffen und eine Situation herbeizuführen, wo Kunden bereit sind, diesen die Chance zu geben, wie Herr Dr. Möllering es so schön ausgeführt hat, Vertrauen auch zu rechtfertigen und hier einen Vorschuss zu geben.

Ich denke aber, dass viele Aspekte, die wir heute gehört haben, rechtliche Fragestellungen usw. im Zeitalter dieses modernen Cloud Computing, wo wirklich riesige Rechnerinfrastrukturen weltweit aufgebaut werden, gar nicht so neu sind und eigentlich schon aufgetreten sind, als das Thema Outsourcing aktuell wurde. Sobald ich IT Leistungen außer Haus gebe, verliere ich einen Teil der Kontrolle über diese Systeme. Ich gebe einem Geschäftspartner Kontrolle über Teile meiner IT. Jetzt ist die Frage, wie stark ich das absichern muss oder wie gut ich das absichern kann. Wo das bisher im klassischen Hosting dadurch gelöst wurde, dass ich mich mit dem Hoster an einen Tisch setze und ggf. auch individuelle Vereinbarungen treffen kann, wird es jetzt im Zeitalter dieses „modernen“ Cloud Computings, wo Rechnerinfrastrukturen in einer Größenordnung da sind, die es einfach erzwingen für diese Anbieter, die Leistungen, die darauf angeboten werden, in einer gewissen standardisierten Form anzubieten. Genau das ist die Situation, vor der auch Microsoft steht.

Wir haben es uns auf die Fahnen geschrieben, eine Plattform bereitzustellen, die generisch genug ist, um möglichst einen großen Markt zu adressieren – natürlich wollen wir möglichst viel Geschäft machen damit –, aber genug Stellschrauben für die Nutzer bietet, um quasi individuelle Anforderungen abdecken zu können. Das ist

ein ganz klassisches Problem, vor dem IT-Anbieter stehen: wie man möglichst industrialisiert, möglichst standardisiert eine Leistung anbieten, aber trotzdem Individualisierungspotenzial bietet. Genau das ist letztlich dieses Spannungsfeld, vor dem auch wir agieren, und wir gehen das insofern an, als dass wir dem Kunden natürlich Stellschrauben im Bereich der Cloud bieten, also auch in Windows Azure zum Beispiel die Möglichkeit, einen Rechenzentrumsstandort zu wählen und wirklich beim Anlegen von Projekten zu bestimmen, dass diese im EU Raum sein und entsprechende rechtliche Anforderungen erfüllt werden müssen. Oder dass wir Standards unterstützen, die eine Interoperabilität mit der Plattform bietet, wo man über Webservices auf die Plattform zugreifen kann. Wie es auch meine Vorredner gesagt hatten, werden Hybridlösungen in Zukunft dominieren, auch aus der Sicht von Microsoft.

Es wird immer Bereiche geben, wo es entsprechende rechtliche Rahmenbedingungen oder andere objektiv messbare Kriterien, also z.B. bestimmte einfach zu erfüllende Paragraphen gibt, oder wo es einfach nur um das Bauchgefühl des Kunden geht, der einfach nicht will, dass seine Daten unkontrolliert irgendwo in der Cloud rumschwirren. Es wird immer Szenarien geben, wo ein Vorortbetrieb oder der Betrieb bei einem ihm bekannten Hoster, wo vielleicht schon ein gewachsenes Vertrauensverhältnis besteht, gewählt wird. Dafür steht Microsoft mit der „Software + Services“-Strategie, indem eine Technologie-Plattform angeboten wird, die durchgängig ist über diese Betriebsmodelle vom Vorortbetrieb über Hosterbetrieb bis hin zur Cloud und der Kunde wählen kann, welches für ihn das bestgeeignete ist, d.h. mit dem die Kundenanforderungen ausreichend abgedeckt werden und daraus kombinierte IT-Lösungen bauen kann.

Prof. Picot:
Vielen Dank, Herr Sirtl. Das war ein schönes Gesamtbild, welches Sie gezeichnet haben. Ehe wir mit Fragen und Kommentaren zum Auditorium übergehen, möchte ich Herrn Prof. Müller fragen, der zuvor referiert hat. Sie haben diese sieben Kommentare aus der Kunden- und auch Anbietersicht gehört. Ich möchte Sie angesichts Ihres Vortrag, der ja das Spannungsfeld zwischen Rationalisierungspotenzial und Kontrollverlust aufgezeigt hat, fragen, ob sich der Schieber dadurch für Sie nun mehr in Richtung Rationalisierungspotenzial oder mehr in Richtung Kontrollverlust bewegt hat oder anders herum gefragt: ist die Wäsche noch grau oder etwas weißer geworden?

Prof. Müller:
Das Erste, was wir ganz klar haben, die Cloud, ist ein Potenzial, das die IT-Dienstleistungen sehr viel billiger anbietet. Das ist für mich eine unumstrittene Tatsache. Die Frage ist, kann man schon oder jemals alles dort rechnen? Herr Auerbach hat 80% genannt. Ich hätte früher 50% gesagt. Aber Cloud kommt; da bin ich total sicher. Darin sind einfach schon zu viele Investitionen getätigt worden und aus Kostengesichtspunkten ist das Modell überzeugend. Es darf sich nur keiner in der

Zeit täuschen. Das ist so wie mit der vorher zitierten Waschmaschine. Wenn Sie die ganz tolle Waschmaschine fünf Jahre zu früh bringen, sind Sie auch schon Pleite, wie wenn sie zu spät kommt. M.E. ist der Kontrollverlust und die noch unbeherrschte Komplexität der Regelschieber. Microsoft gibt 4 Milliarden aus. IBM gibt auch viele Milliarden, ebenso wie Google und Amazon, SAP denkt jeden Tag darüber nach, was sie tun sollen. Stellen Sie sich vor, dass Cloud kommt und SAP ist nicht dabei. Dann ist SAP erledigt. Kommt Cloud nicht und SAP hat darauf gesetzt, ist SAP auch pleite. Die Geschäftsprozesse werden enorm schwierig zu transferieren sein, denn das betrifft Zehntausende von Mitarbeitern. Wenn ich eine Wette machen müsste, würde ich sagen, dass Cloud kommt.

Prof. Picot:
Vielen Dank, Herr Müller. Ich darf jetzt Sie alle einladen, Ihre Fragen und Kommentare an das Podium zu richten, denn ich kann mir vorstellen, dass im Laufe des Tages das eine oder andere noch offen geblieben ist. Bitte sehr, Frau Kollegin Stopka.

Frau Prof. Stopka, TU Dresden:
Ich bin dem Panel erst einmal sehr dankbar, dass Sie die wirtschaftlichen Probleme intensiv aufgegriffen haben, nachdem wir heute Vormittag mehr die sicherheitsrechtlichen Dinge diskutiert haben. Herr Dueck erwähnte, dass sich die intensive Nutzung des Cloud Computing vor allem aus dem Kosteneinsparungszwang bei den Anwendern, den nachfragenden Unternehmen entwickeln wird. Aus dem Motiv der Verlagerung von Rechen- und Speicherleistungen auf Serverstrukturen von Cloud Computing Dienstleistern ergeben sich bei diesen die entsprechenden Erlöspotenziale. Könnte man zum heutigen Zeitpunkt schon ein paar Gedanken zu den Erlösmodellen der Anbieter für Cloud Computing Dienstleistungen vorstellen oder ist das noch zu früh?

Prof. Picot:
Das ist eine sehr legitime und wichtige Frage. Wir haben gerade gehört, Geschäftsmodelle kommen und gehen. Hier kommt eins. Wollen wir einmal schauen, wie es aussieht. Was sagen Sie dazu? Zu jedem Geschäftsmodell gehört ein Erlösmodell. Bitte sehr, Herr Dueck!

Prof. Dueck:
Ich gebe Ihnen ein Beispiel. Der Kunde kommt und alle sagen, dass sie das genauso wie Amazon haben wollen, pay per use, sekundengenaue Abrechnung. Davor fürchtet sich unter Umständen die IBM, weil die Einnahmen aus den Cloudlösungen dann schwer kalkulierbar sind. Unsere Kunden könnten mehr oder weniger „Cloud“ verbrauchen und auch sofort den Anbieter wechseln. Das ist für Kunden kein Problem, wenn man mehrere Cloud Anbieter hat. Die Anbieter möchten natürlich lieber mit dem Kunden einen Mindestabnahmevertrag oder eine Flatrate vereinbaren, also streitet man sich. Es geht wahrscheinlich so aus, dass die

Kunden eine genaue Abrechnung durchsetzen, weil ihnen das zuerst von den Kosten her vorteilhafter erscheint. Dann aber wird der CFO des Kunden irritiert die ständig wechselnde Rechnungshöhe sehen und sich vor dem unkalkulierbaren Risiko der Rechnungshöhe fürchten. Wahrscheinlich wird man deshalb im Cloud Computing dann doch wieder Flatrates sehen, so wie im privaten Umfeld auch, wo wir fast alle bei Telefon und DSL Flatrates haben, weil uns die sekundengenaue Abrechnung bei der Nutzung nervös macht.

Wir wissen heute alle, dass die Flatrate eventuell zu teuer ist, aber wir sind emotional ganz ruhig dabei. Bevor sich aber die Flatrate-Tarife durchsetzen, kann es sein, dass Cloudanbieter zuerst sündhaft teure Billingsysteme entwickeln und bauen, die später nicht mehr gebraucht werden. Was machen wir jetzt mit den Investitionen? Das hat Günter Müller gerade gesagt. Man muss sich jetzt irgendwie in die Entwicklung hineintasten. Das ist eine spannende Frage: Wie ist das Nutzungsverhalten der Kunden, wie viel Speicher brauchen sie für Mails, wie oft sind sie online? Google bietet zum Beispiel mehr Mail-Speicher an als ein normaler IBM Mitarbeiter überhaupt auf der Platte haben sollte. Wir bieten deshalb andere Modelle an. Dann werden Sie sagen, dass die IBM immer so wenig Speicher bietet. Das brauchen die Mitarbeiter ja nicht, weil es eine Dienst-Email ist usw. Das gegenseitige Belauern der Hersteller und der Kunden führt langsam zu mehr Einigkeit. Alles wird sich einspielen, und das dauert einfach ein paar Jahre.

Noch eine Bemerkung: Angenommen, ein Anbieter baut eine riesige Cloud, die zum Beispiel einen Speicherpreis von 6 Cent den Monat für 1 Gigabyte möglich macht. Dann gibt es eine Revolution in der Speichertechnik – und man kann vielleicht die Leistungen den Kunden zum halben Preis anbieten. Was geschieht dann mit den alten Cloud-Fabriken? Sehen Sie das Risiko? Günther Müller hat ja gerade gesagt, wer da zu früh reinkommt und einen zu hohen Preis macht, weil er eine alte Technologie nimmt, den beißt es. Das ist richtig hart. Und deswegen plädiere ich dafür, das alles ein bisschen evolutionär zu sehen. Seien wir nicht so ungeduldig und nehmen wir uns die Zeit zu sehen, dass da viele Schwierigkeiten und Unwägbarkeiten zwischen den Anbietern und den Nutzern sind. Das alles bekommen wir aber demnächst hin. Das ist nur so ein Einrütteln.

Prof. Picot:
Aber hier gibt es jemand, der über lange Zeit schon sehr viel Erfahrung damit hat. Herr Leistenschneider, wie macht das Ihre zugegebenermaßen relativ geschlossene, aber doch sehr große Gruppe, zugleich mit langjähriger Erfahrung? Was haben Sie für ein Erlösmodell? Sie müssen ja auch von irgendwas leben?

Herr Leistenschneider:
Wir haben ein sehr ausgeprägtes Preismodell. Wir haben dieses Preismodell 1995 eingeführt und berechnen für die Überlassung unserer Software monatliche Überlassungsvergütungen statt Einmalpreise.

Prof. Picot:
Ist das eine Lizenz?

Herr Leistenschneider:
Das ist eine Überlassungslizenz, in der die Softwarewartung mit allen Updates etc. enthalten ist. Unsere Steuerberater und deren Mandanten brauchen nicht zu befürchten, plötzlich und unerwartet ein kostenpflichtiges Software-Update zu bekommen, wofür sie Geld auf die Seite legen müssten. Dies alles ist mit den monatlichen Überlassungsvergütungen abgegolten.

Prof. Picot:
Die Daten spielen keine Rolle?

Herr Leistenschneider:
Doch, da komme ich noch dazu. Die kommen noch einmal extra. Das ist so austariert, weil es ja Kanzleien gibt, die ein sehr hohes Datenvolumen haben und welche, die nur ein kleines haben. Am besten zeigt sich das beim Lohn. Da wird pro Arbeitnehmer im Prinzip abgerechnet oder wenn gedruckt wird, pro Druckzeilen oder wenn übermittelt wird, gibt es da auch Datenvolumina, die die Grundlage bilden. Aber das spielt sich alles im Nachkomma-Centbereich ab.

Prof. Picot:
Und bei Google, wie läuft es da mit Ihren Preisstrukturen oder Konzepten?

Herr Gutzeit:
Flatfee, das heißt 40 Euro pro Nutzerkonto pro Jahr und 25 Gigabyte E-Mail-Kapazität. Den Unternehmen stehen zudem Rund-um-die-Uhr-Support, zusätzliche Backend-Funktionalität sowie Integrationsdienste zur Verfügung. Die Bausteine der Google Apps Premier Edition sind im Einzelnen: Google Mail, der gemeinsam nutzbare Google Kalender, Google Text & Tabellen für Dokumente, Tabellenkalkulationen und Präsentationen, das schon erwähnte Tool Google Video, Google Talk für Instant Messaging, Chat und Telefonie über das Internet und Google Sites zur Erstellung eigener Webseiten. Vor Kurzem haben wir für Google Text & Tabellen die Möglichkeit hinzugefügt, jedes beliebige Fileformat hochzuladen. Dabei erhält jeder Nutzer 1 GB Speicherplatz, und jede einzelne hochgeladene Datei darf bis zu 250 Megabyte umfassen.

Prof. Picot:
Und Windows Azure, wie geht das? Das kann man sich sogar im Internet anschauen, was Sie da für ein Preisschema haben.

Herr Sirtl:
Genau. Es ist alles letztlich über die Webseite einsehbar. Wir rechnen da auch bestimmte IT Größen ab, sei es Gigabyte Datentransfer usw. Aber ich denke, es ist

insofern eine interessante Fragestellung, als dass viele Anbieter – der Kollege von Google hat es auch gerade gesagt – in technischen Einheiten abrechnen. Was aber viele Firmen interessiert, sind eher businessorientierte Abrechnungseinheiten. Was kostet mich wirklich der User? Oder was kostet mich ein Monat „E-Mail-Machen". Viele wissen vielleicht gar nicht, wie viele Transaktionen ihre Emailnutzung vielleicht auf dem Cloud System verursacht. Von daher ist es durchaus eine Herausforderung für die Anbieter, auch ein vernünftiges Mapping von IT- Größen, die gerade noch Systemadministratoren überschauen können, in Businessgrößen zu machen, die dann letztlich für die Anwender relevant sind, weil die eben nutzungsabhängig abgerechnet werden wollen.

Prof. Picot:
Vielen Dank. Wenn ich auch noch Herrn Auerbach fragen und das gleich mit einer weiteren Frage verbinden darf. Wir haben über Preise gesprochen, aber Preise ohne sonstige Konditionen sind oft nicht so aussagekräftig. Was geben Sie denn für Sicherheit oder Garantien oder anders herum für Haftungsversprechen, wenn irgendetwas nicht funktioniert, abgesehen vom Preisschema?

Herr Auerbach:
Zunächst zum Preisschema: es ist total spannend, dass sehr viele Dienstleistungen im Endkonsumerbereich fremdfinanziert sind. So kostet die normale Mailbox nichts, die meine Kinder oder auch sie nutzen. Sie ist über Werbung querfinanziert. Des weiteren gibt es so genannte Bundle-Angebote, in denen sie IP TV, das Festnetz, das Mobiltelefon und den Datenstrom in einer Flat-Fee kombinieren. Dadurch können Sie gar nicht mehr unterscheiden, was zahlen sie eigentlich für welche Dienstleistung. Auch wandern zunehmend IT-Dienstleistungen mit hier hinein. Wenn sie dieses Paket nun auch noch mit Werbung oder sonstigen Dingen, wie verbilligte Endgeräte querfinanzieren, bleibt es sehr spannend die Angebote untereinander vergleichbar zu machen.

Welche Garantien geben wir? Im Endkundenbereich sind das ganz normal die allgemeinen Geschäftsbedingungen. Die kann man überall nachlesen und sie gelten nahezu gleich für unsere Standardprodukte. Im Geschäftskundenbereich sind die rechtlichen Bedingungen identisch mit denen von klassischen Outsourcing Verträgen. Da wird im Prinzip nicht unterschieden, ob das Produkt jetzt auf einer Cloud produziert wird oder in klassischen Umgebungen. Haftung und Gewährleistung sind hier sind hier vergleichbar.

Prof. Picot:
Wir haben heute Morgen von Dr. Möllering gehört, dass es in einem vertrauensgetriebenen Geschäft wichtig ist, die Verantwortung kompetent wahrzunehmen und verantwortlich auf die Erwartungen zu reagieren. Wenn ich mir jetzt vorstelle, dass zum Beispiel ein junges Start up sein Geschäftsmodell sehr stark z.B. vom Funktionieren der Cloud von Google abhängig macht, und auf einmal funktioniert die

Cloud aus irgendwelchen Gründen ein, zwei Tage nicht mehr. Dann kann diese wunderbare Kurve nicht mehr so hoch gehen, wie wir es vorhin gesehen haben, und dann kann unter Umständen ein ganzes Lebenswerk zusammenbrechen von jungen Leuten, die monate- und jahrelang daran gearbeitet haben, ein Geschäftsmodell aufzusetzen. Ich habe gehört, dass dann die Haftungssumme, die zur Verfügung steht, relativ oder vernachlässigbar gering ist, die dann von Seiten der Cloud Anbieter geboten wird. Hier haben wir dieses Vertrauensverhältnis mit den gewissen Erwartungen. Wie gehen Sie damit um? Können Sie dazu etwas sagen, Herr Gutzeit und die anderen hier?

Herr Gutzeit:
Natürlich beinhalten unsere Verträge mit Geschäftskunden gewisse Haftungsklauseln, ganz klar. Aber wir sind von unserer Technologie und der Sicherheit unserer Datenzentren beziehungsweise ihrer Skalierbarkeit so überzeugt, dass wir mit Sicherheit sagen können, dass Sie zwei Tage Ausfälle nicht erleben werden. Solch ein Vorfall würde die ganze Cloud Computing-Thematik ad absurdum führen und Kunden aus genau diesem Grund dann nicht zu uns oder zu IBM oder zu Microsoft führen. Deswegen liegt es uns sehr stark am Herzen, diese Verfügbarkeit durch Service Level Agreements zu gewährleisten. Für unsere Google Apps Premier Edition beispielsweise garantieren wir eine Verfügbarkeit von 99,9 Prozent pro Jahr. Und natürlich sind wir daran interessiert, dass mehr und mehr Kunden zu uns kommen. Es bietet sich gerade hier an auch noch einmal auf das Thema Sicherheit zurück zu kommen: Wir bei Google tun alles dafür, dass die Cloud verfügbar und sicher ist. Wir haben unter Anderem gewisse Redundanz-Mechanismen in unseren Datenzentren, die selbst bei einem potenziellen Flugzeugabsturz auf eines der Datenzentren verhindern, dass unsere Kunden mit Ausfällen von Tagen oder Stunden konfrontiert sind. Wenn einmal etwas ausfallen sollte, dann handelt es sich um maximal minutenlange Störungen, die umgehend behoben werden und dank unserer redundanten Systeme umgangen werden können.

Prof. Picot:
Der Strom kommt aus der Steckdose sozusagen. Wunderbar. Jetzt habe ich hier eine Wortmeldung von Herrn Hertz.

Herr Hertz, IBM Deutschland:
Wir sind von anderen Versorgungsleistungen gewohnt, dass wir Anbieter wechseln können. Inwieweit spielt die Wechselmöglichkeit bei IT-Versorgern in der Zukunft eine entscheidende Rolle und was sind Maßnahmen, mit denen dann diese Wechselmöglichkeiten geschaffen werden? Wie sieht es aus mit Standardisierung, insbesondere auf Geschäftsprozessebenen und nicht nur in der technischen Infrastruktur? Wie sieht es beispielsweise aus, wenn ich Terabyte an Daten von einem Mailprovider zum anderen bewegen will? Das geht ja nicht mehr nur über das Netz. Werden dann Festplatten verschickt?

Prof. Picot:
Vielleicht würden Sie als sehr großer Akteur eine Antwort versuchen, Herr Gutzeit, und dann vielleicht von den anderen jemand. Bitte schön!

Herr Gutzeit:
Wir reden bei unserem Cloud Computing-Produkt Google Apps, einer Messaging & Kollaboration-Plattform, von allem, was mit E-Mail, Instant Messaging, Texterstellung, Dokumentenerstellung etc. in der Wolke zu tun hat. Und wir haben bei Google eine dedizierte Initiative ins Leben gerufen, die Sie auch im Web nachlesen können, und die wir die Data Liberation Front nennen. Diese Initiative hat ein Produkt entwickelt, das Benutzern ermöglicht, alle ihre Daten, die sie bei Google hinterlegt haben, mit ein paar wenigen Klicks wieder komplett mitzunehmen. Das ist eine Initiative von Google, die einzigartig ist. Und alle unsere Programmierer und Ingenieure haben als Maßgabe, Produkte nach den Grundsätzen der „Datenbefreiung" zu entwickeln und zu programmieren. Unsere gesamte Architektur ist als offenes System gestaltet, sodass über APIs sämtliche Protokolle und Bereiche auch unserer Google Apps Premier Edition offen gestaltet sind. Wir wollen es unseren Kunden ermöglichen, wenn sie nicht mehr bei uns bleiben wollen, mit diesen wenigen Klicks ihre Daten in jeder Form, Art und Weise wieder mitzunehmen. Das spornt uns natürlich an, alles Mögliche für den Verbleib unserer Kunden bei Google zu tun.

Ich habe eben über Verfügbarkeiten gesprochen. Ich habe über Preise gesprochen. Ich habe über Sicherheit gesprochen. Ich habe über Innovationen gesprochen. All das ist für uns Ansporn und Motivation dafür, dass uns unsere Kunden eben nicht mit ein paar Klicks verlassen, sondern bei uns bleiben. Da ist auf der technologischen Seite sicherlich noch einiges möglich. Vor einigen Monaten wurde auf einem Vortrag speziell über die Vernetzung von verschiedenen Wolken – beispielsweise zwischen einer IBM Wolke und einer Google Wolke – gesprochen, sodass man als Kunde seine Daten hin- und hertauschen kann. Ich denke, das ist noch Zukunftsmusik. Aber sicherlich macht sich der eine oder andere schon Gedanken darüber.

Prof. Picot:
Ich kann mir vorstellen, dass ein solcher Wechsel gerade für große Unternehmensanwendungen überhaupt keine triviale Angelegenheit ist. Vielleicht ist das bei hoch standardisierten Anwendungen möglicherweise einfacher, aber wenn es in die Unternehmensspezifika geht, bei Enterprise Ressource Systemen usw., die über die Cloud abgewickelt werden, kann ich mir einen Wechsel – eine verständliche Anforderung – als sehr komplex vorstellen. Wir sieht das aus, Herr Auerbach?

Herr Auerbach:
Ich würde noch einmal kurz auf die ganz einfache Mail eingehen. Ich glaube, dass es kommerziell möglich ist, per Mausklick von einem zum anderen zu wechseln. Nehmen wir einen Kunden, der mehrere hundert Mitarbeiter hat. Alle haben eMail-

boxen mit Historie, entsprechende Tabellenkalkulations- und Schreibsystems, um es neutral zu formulieren. Wenn sie nun von einem Provider wie Notes, Google oder Microsoft hin- und herwandern wollen, ist das kommerzielle Problem das Geringste.

Wenn ich mir allein anschaue, was es schon bedeutet, wenn ich von Windows 2007 auf 2009 gehe und ein Worddokument zweimal hin und zurück umwandle. Eine komplexe Excel hoch und runter verwandele oder eine Powerpoint-Datei mit Animation. Das kann man nachher nicht unbedingt wiedererkennen. Und wenn ich das gleiche zwischen den Welten Cloud und normaler hin- und her shifte, kann es weg sein. Dies ist die eigentliche Schwierigkeit.

Man muss sich bewusst sein: gehe ich in eine Cloud findet auch eine gewisse Festlegung auf den Anbieter statt. Dies erachte ich aber als geringes Problem, weil ich die neutrale Leistung, nämlich ein Schreibsystem oder ein Tabellenkalkulationssystem haben möchte. Ich kann sie vergleichen, da sich aus meiner Sicht die drei Systeme funktional nicht grossartig unterscheiden, zumindest was den Tagesbetrieb angeht. Insofern ist die Wettbewerbsfähigkeit gegeben und ich gehe davon aus, dass die Server vergleichbar sein werden. Es wird weder qualitativ, funktional noch wirtschaftlich großen Druck geben, dann einen Wechsel zu vollziehen.

Prof. Dueck:
Wir haben bei LotusLive zusätzlich noch viele Collaboration Tools mit drin, auch so eine Art Facebook. Das wird alles mitgeliefert, mit dem kompletten sozialen Netzwerk. Wenn man in eine andere Mail-Cloud wechselt, wird das alles dort anders ein, mit anderen Community Tools. Da werden sich die Leute nicht umgewöhnen wollen. Ich denke deshalb, dass man nicht wirklich hektisch die Anbieter wechselt, eher nur damit droht und Preise verhandelt.

Dr. Götz, Detecon:
Wir haben etwas gehört über komplexe Anforderungen aus dem Geschäft großer Unternehmen. Wir sind uns auch alle einig, dass der Cloud Computing Markt eigentlich nur dann gesund wächst, wenn er sich von Infrastructure as a Service lösen und sich in Richtung hochwertiger Applikationsleistungen, d.h. Software as a Service, entwickeln kann. Sonst haben sie gar keine relevanten Angebote für große Unternehmen. Der einzige, der das differenziert adressiert hat, war Herr Auerbach. Herr Auerbach sagt zu Recht: Mit komplexen Anwendungen und Datenstrukturen spielt man in einer anderen Liga. Die ganze Diskussion der letzten 10 Minuten behandelt aber nur Infrastruktur, Plattenplatz, Mail, aus reiner Anbieter- und Verkaufssicht, und jeder von Ihnen weiß, dass sie damit ihre großen Investitionen in Cloud Computing gar nicht refinanzieren können. Ich habe den Eindruck, demnächst bekomme ich noch eine Yucca Palme zum 5€-Mail-Vertrag gratis dazu. Das ist doch nicht die Frage, über die wir hier sprechen sollten. Wir sollten doch eher über die Frage diskutieren, wie man zum Beispiel einen fairen Preispunkt für Software as a Service findet, um komplexere Unternehmensapplikationen abzudecken.

Wie ist die Refinanzierung der Investitionen unter Berücksichtigung der Randbedingungen des Datenschutzes etc. anzusetzen? Dazu erhoffen wir uns eine Antwort und nicht, ob ich 40, 30 oder 5 Euro für ein Mail Account bezahlen darf – obwohl ich die Yucca Palme gern mitnehmen würde. Aber im Ernst: Wenn sich die Preisstrukturen so entwickeln sollten wie Sie das hier dargestellt haben, dann bleibt letztendlich nur die „alles-fast-umsonst"-Todesspirale übrig, in der sich heute etliche andere low-ARPU Geschäftsmodelle befinden. Deshalb meine Frage: Was tun Sie aktiv, um im Bereich hochwertiger Unternehmensapplikationen das Software as a Service Geschäft substanziell und gesund aufzubauen?

Prof. Picot:
Herr Sirtl, bitte schön!

Herr Sirtl:
Eine sehr interessante Frage, insbesondere weil sie auch so ein bisschen den Bogen schlägt zur vorhergehenden Frage hinsichtlich Standardisierungen. Also, vielleicht der kurze Umweg, bevor ich zur eigentlichen Antwort komme. Ich denke tatsächlich, dass viele Angebote so von unten, Infrastructure, Plattform, Software langsam nach oben wachsen, weil einfach auf den unteren Schichten die Standardisierung deutlich weiter fortgeschritten ist. Wenn ich in den Software as a Service Bereich gehe, ob ich jetzt einen CRM von Salesforce mit einem Dynamics Online vergleiche, ist die Vergleichbarkeit sehr viel schwieriger zu machen und auch die Standardisierung da weniger fortgeschritten. Was wir in dem Zusammenhang machen, ist, dass all unsere Systeme letztlich, selbst wenn wir eine proprietäre Lösung hinstellen mit einem Dynamics Online, was es eben nur bei Microsoft gibt, aber dann das Ganze über Webservices entsprechend so zugreifbar zu machen, dass ich jederzeit an meine Daten rankomme und dann auch eine Migration in anderen Wolken ermögliche, dass ich die Daten rausziehen kann. Aber ich stimme meinen Vorredner zu; es wird in gewissen Schichten immer schwierig sein, 1:1 Dinge aus der einen Wolke in die andere reinzusetzen, weil einfach – wie ich es auch in meinem Kurzvortrag gesagt hatte – immer dieses Spannungsfeld zwischen Standardisierung und Anpassbarkeit besteht. Dies bedingt auch, dass ich den Programmierern vielleicht Vorgaben mache, wie sie ihre Software zu schreiben haben, damit sie in meiner Wolke optimal laufen, aber vielleicht nicht in der Wolke vom Anbieter B. Anders sieht es mit den Daten aus. Datenstrukturen lassen sich relativ leicht rausziehen, auch bei uns: auf SQL Azure ziehen Sie die Daten ohne Probleme mit einem SQL Tool raus und können Sie dann in andere relationale Datenbanken importieren. Aber was wir tun, um das auch auf den höheren Schichten zu machen, ist, alle unsere Produkte, die wir im Onlinebereich anbieten, Webservices-konform auch zu öffnen, so dass sie abgreifbar sind von Tools, die Datenexport und -migration zu anderen Clouds ermöglichen.

Prof. Dueck:
Ein typisches Problem ist das Sizing von SAP-Lösungen, was einen echten Meister verlangt. Für so viele tausend Arbeitsplätze braucht man soundso viele Server, so viel Speicher usw. In einer Cloud müsste so eine Lösung aber nicht auf festen Ressourcen laufen, sondern im Falle des rapide wachsenden Unternehmens im Beispiel von Günter Müller mit der Flut der neu hereinkommenden Kunden mitwachsen und sich auf der Cloud ausbreiten. Wenn am Wochenende das Unternehmen eventuell schließt, müsste sich auch die Software dafür langsam schlafen legen bzw. auf ein Mindestmaß schrumpfen, also die Ressourcen freigeben. Heutige Software macht das in der Regel leider nicht mit. Wir bei IBM bauen derzeit Managementschichten in WebSphere ein, die ein solches Atmen der Ressourcenumgebungen erlauben. Dieser Umbau der Software für die bessere Cloud-Tauglichkeit braucht einen langen Atem – das geht nicht so schnell, bei vieler Software eventuell gar nicht.

Zusätzlich gibt es noch viele ungelöste Lizenzierungsfragen bei Software. Also etwa: wer zahlt für welchen Computer wie viel Lizenz? Wenn eine kleine Software immer auf anderen CPUs in der Cloud benutzt wird – werden dann ebenso viele Lizenzen fällig? Das ist hier noch nicht angeklungen. Es müssen so viele Probleme noch gelöst werden. Das ist nicht so einfach. Da will ich mich hier nicht hinstellen und sagen, dass wir das alles nächstes Jahr liefern können.

Prof. Picot:
Das sind noch einmal wichtige Hinweise gewesen, dass die Softwaresysteme sich dem auch anpassen müssten einschließlich der Lizenzmodelle – eine wichtige Thematik. Ich möchte vorschlagen, dass wir diejenigen Fragen, die noch im Raum sind, sammeln und dann beantworten. Ich sehe noch drei Wortmeldungen.

Dr. Möllering:
Ich finde die Diskussion äußerst spannend und möchte gern noch einen Kommentar und eine Frage aus der Sicht der Vertrauensforschung anbringen. Ich finde es sehr interessant, dass Sie darauf verwiesen haben, dass in einigen Jahren das Cloud Computing wahrscheinlich ganz selbstverständlich sein wird. Aus meiner Sicht aus der Forschung ist es etwas ganz Typisches für Vertrauen, dass man vertraut, weil es selbstverständlich ist und weil andere auch vertrauen. Allerdings dürfen wir nicht vergessen, dass Cloud Computing heute noch nicht selbstverständlich ist. Wir sind in einer frühen Phase. Wir sehen hier auf dem Podium die Vorreiter in dieser Bewegung. Da finde ich es schon bedenklich, wenn man auf die Selbstverständlichkeit in der Zukunft verweist. Da müsste man heute anders argumentieren. Ich erinnere noch einmal an die in meinem Vortrag angesprochene Rolle der Stewardess als Zugangspunkt zu einem abstrakten System. Eine Stewardess kann zu einem Fluggast mit Flugangst nicht flapsig sagen: „Sie können ja auch mit dem Auto fahren“ oder „Ach, wir sind noch nie abgestürzt“. Da muss man sich schon besonders bemühen, das Vertrauen aufzubauen, und kann nicht auf etwas Selbstverständliches verweisen, was noch nicht selbstverständlich ist. Von daher sind Sie aktuell in einer

besonderen Rolle, gerade die Provider, die immer wieder demonstrieren, dass es funktioniert. Zweitens ist mir heute insgesamt aufgefallen und auch jetzt in dieser Runde noch einmal, dass wir oft die Vertrauensproblematik irgendwohin verschieben und dann einer gewissen Kontrollillusion verfallen. Und zwar war es einmal der Staat, der einspringen sollte, und damit sei das Problem gelöst – aber eigentlich ja nur verschoben eben zum Vertrauen in den Staat. Dann die Versicherungen: eine sehr interessante Lösung, aber eigentlich auch nur eine Verschiebung der Vertrauensproblematik hin zu den Versicherern. Ebenso die neuen Protokolle und Zertifikate, die Vertrauen möglich machen sollen, aber selbst Vertrauen verlangen. Ich sehe da vor allen Dingen immer eine Verschiebung des Vertrauens in ein anderes Objekt, und das Vertrauen bleibt immer noch problematisch. Hier und heute haben die Provider den Eindruck erweckt, dass sie im Cloud Computing alles unter Kontrolle haben. Es ist sehr wichtig, dass Sie das betonen, aber dennoch frage ich mich, wem denn dann die Provider vertrauen. Wenn also die Kunden bereit sind, den Providern zu vertrauen, auf wen verlassen sich dann wiederum die Provider? In wen setzen Sie Ihr Vertrauen, dass Sie auch über viele Jahre hinweg die Systeme weiterentwickeln können und zum Beispiel auch technologisch weiter in der Lage bleiben, alles zu beherrschen, wenn sich das Cloud Computing immer weiter ausbreitet und immer mehr Kunden es nutzen.

Prof. Picot:
Vielen Dank. Dort war eine Meldung.

Herr Söllner, TU München:
Es ging ja hier um Vertrauen in IT und ich möchte meine Antwort auf die Frage, die wir hier vorne hatten, so geben, wie ich das mitgenommen habe und Ihre Einschätzung dazu gern wissen. Wann vertrauen Sie Ihr Geschäft der Internet Cloud an? Meine Antwort wäre darauf; sobald Faktoren der Sicherheit, des Mehrwerts, der Kostenersparnis hoch genug sind, damit ich es einfach nutze, auch wenn ich kaum Vertrauen darin habe. Und das Vertrauen bildet sich dann quasi, wie Herr Sirtl gesagt hat, über die Zeit hinweg durch die funktionierende Nutzung. Wäre das so richtig?

Prof. Dueck:
Ganz kurz, wenn Sie Kodakfilme zur Entwicklung geben und sie mit tiefem Bedauern schwarz zurückbekommen, wenn also zum Beispiel die heiligen Hochzeitsbilder versaut sind, dann bekommen Sie 6,99 € Schadenersatz für den Film. An diese Regelung haben wir uns gewöhnt, weil das eigentlich nicht so oft passiert, vielleicht jedem einmal im Jahrzehnt und das nehmen Sie hin. Das wird sich langsam genauso auch bei Cloudpannen einspielen.

Prof. Picot:
Bitte noch eine abschließende Frage und dann gehen wir in die Schlussrunde.

Herr Decker, Journalist:
Ich habe eine Frage von der sprachlichen Seite her. Mich hat von Anfang an der ganzen Diskussion, nicht nur heute sondern bereits seit einem Jahr der Begriff Cloud fürchterlich irritiert. Warum ist eigentlich aus einem Netz eine Wolke geworden. Eine Wolke ist doch eigentlich etwas Diffuses, etwas völlig Unterschiedliches. Komischerweise sprechen wir nicht von einer sozialen Wolke sondern von einem sozialen Netz, was ja auch in Ordnung ist. Man sitzt auf einer Wolke, vielleicht der Wolke 7. Aber ansonsten ist es alles ziemlich undurchsichtig. Meine Frag ist: Beabsichtigt eigentlich die gesamte Wirtschaft aus dieser Wolke wieder ein Netz zu machen, wie ich es von Microsoft höre. Das ist ja vollkommen in Ordnung. Auch manche Telekoms gehen dazu über, wieder ein überschaubares Netz zu machen, damit ich genau weiß, wo meine Daten liegen. Interessanterweise hat Herr Gutzeit gesagt, dass nicht einmal er weiß, wo die Daten eigentlich sind. Mich erschreckt das, und von da aus sehe ich überhaupt keine Chance, Vertrauen zu gewinnen, denn bei einer Wolke bin ich im Nebel, bin ich im Undurchsichtigen. Ich werde mich selbst nicht positionieren können. Meine Frage: wohin soll es gehen? Zur Genauigkeit oder ist es ganz praktisch, dass das Ganze so diffus geworden ist?

Prof. Picot:
Vielen Dank. Wollen Sie gleich beginnen mit den Punkten, die Sie gerne aufgreifen möchten?

Herr Gutzeit:
Ich fand sehr interessant, was Sie gerade angesprochen haben. Heute machen wir uns keine Gedanken mehr darüber, wo der Strom herkommt. Der kommt aus der Steckdose, fertig. Dass auch wir als Cloud Computing-Anbieter gewisse Gesetzgebungen einhalten müssen, ist selbstverständlich. Man fragt sich vielleicht bei diesem Thema eher, woher die Leistungen stammen. Viele von Ihnen sind schon seit vielen Jahren mit der IT-Branche vertraut und wissen, dass wir früher, wenn wir über das World Wide Web oder das Internet gesprochen haben, häufig eine Art Wolke gezeichnet haben, die via Router und so genannte Switches irgendwie in das Internet verbinden sollte. Das war der Ursprung von Cloud Computing.

Herr Auerbach:
Aus meiner Sicht noch einmal etwas ganz Simples. Alle, wie wir hier sitzen, sind darauf angewiesen, dass wir Komplexität reduzieren. Wir benutzen so viele Dienstleistungen. Dieses Mikrofon, den Strom, das Flugzeug, mit dem ich nachher heim fliege usw. Ich habe keine Ahnung, wie es funktioniert. Ich verlasse mich voll darauf. Wir haben in der ganzen Bundesrepublik für die eben aufgezählten Dinge hier etwa hundert Spezialisten, die wirklich wissen, wie jedes einzelne im Detail funktioniert und die es weiterentwickeln können. Wir verlassen uns zu 100% auf sie. Das sind wir alle gewohnt. Wir haben keine andere Chance, weil wir selbst irgendwo in Spezialgebieten arbeiten, in denen nur wir uns auskennen. Ich bin dann

darauf angewiesen, dass die anderen mir zuarbeiten, dass ich mich auf sie verlassen kann.

Meine Kinder haben kein Problem damit. Wenn ich denen heute Abend erzähle, was wir hier heute diskutieren haben, gucken die mich mit großen Augen an und fragen, was ich eigentlich für ein Problem habe. Die Komplexität und die Fragestellung ist einigen wenigen vorbehalten, die sich tatsächlich auch mit den negativen Auswirkungen befassen. Aber die Mehrheit, 99% der Bevölkerung denkt überhaupt nicht darüber nach. Davon bin ich fest überzeugt.

Das geht in eine Richtung und wird selbstverständlich wie diese Beispiele, die Sie vorhin genannt haben. Da wird der Weg richtig sichtbar, den wir gehen werden. Diese Entwicklung muss begleitet werden durch Gesetzgebung. Muss begleitet werden durch Versicherung, durch Rechtsanwälte, aber mit einem vernünftigen Aufwand und mit der richtigen Gewichtung.

Prof. Dueck:
Ich würde sagen, dass Anbieter sich einfach keinen Vertrauensschaden leisten können. Der eigene Shareholder-Value nimmt bei einem großen Ausfall erheblichen Schaden. Das riskiert kein Anbieter.

Prof. Picot:
Herr Müller.

Prof. Müller:
Ich will noch einen seltsamen Gedanken beitragen, zu dem Herr Dr. Götz mich provoziert hat. Ich glaube nicht, dass die Büro- und Geschäftsprozesse die ersten sein werden, die Cloud rechtfertigen. Das war zur Zeit der 60er Jahre der Fall, als die IBM den großen Rationalisierungsschub ausgelöst hat. Wir hatten das schon einmal – ich weiß nicht, ob es sich wiederholt – Microsoft hat auch nicht gewonnen mit seinen phantastischen Geschäftsanwendungen sondern mit Computerspielen. M.E sind es wieder die Computerspiele, die das Modell für die Refinanzierung von Cloud ausmachen werden.

Herr Gutzeit:
Wenn ich die Frage von Herrn Dr. Möllering noch einmal aufnehmen darf in Bezug auf Vertrauen. Wie gewinne ich denn das Vertrauen? Vor vielen Jahren hat Ihre Urgroßmutter das gesparte Geld unter das Kopfkissen gelegt. Heute sehen wir es gar nicht mehr. Die Gehaltsschecks gehen ganz automatisch an die Banken und wir bezahlen mit Kreditkarte. Das ist ganz normal. Darüber denkt heute kein Mensch mehr nach. Das Vertrauen ist gewachsen. Aber das Gespräch damals mit Ihrer Urgroßmutter hat sicherlich ein erster Banker geführt, der sie langsam aber sicher durch Erklärungen dahin geführt hat, dass sie es einmal ausprobiert. Vielleicht nicht mit ihrem ganzen Gesparten, sondern nur mit einem Teil. So konnte sie sehen, was passiert und dass sie dem Banker vertrauen kann und einen Mehrwert für sich

erzielt. Genau das ist der Ansatz, den ich mit anderen Vertriebsmenschen gemein habe und ich sage: Lasst uns mit den Kunden sprechen. Ich erwarte nicht, dass die gesamte UBS Bank morgen alles in die Cloud stellt und 110.000 Mitarbeiter sofort ihre Kommunikation und Kollaboration über Google's Platform erledigen, aber vielleicht einen Teilbereich davon. Man könnte beispielsweise mit einem Unternehmensbereich den Weg in die Cloud gehen, der mit weniger geschäftskritischen Daten agiert, und so herausfinden, ob das Cloud Computing-Modell dem Unternehmen Mehrwert bietet. Das ist unsere Aufgabe als Anbieter, dem potenziellen Kunden diese kleinen Schritte in einem Gespräch näher zu bringen. Und unsere Vertriebsteams, die Sie per Telefon oder persönlich vor Ort beraten, sind speziell dafür geschult, mit Ihnen sowohl über die kleinen als auch die großen Schritte zu sprechen, mit Ihnen die Verträge durchzugehen und mögliche Schwierigkeiten zu erkennen und Lösungsansätze zu liefern. So gewinnt man Vertrauen. Sicherlich ist das kein leichter Weg, er ist aufwendig und es wird noch eine Weile dauern, bis das Vertrauen in die Wolke gefestigt ist. Dennoch können Cloud-Anbieter wie wir schon jetzt sagen: „Schau mal, wen wir schon als Kunden gewonnen haben. Darunter sind Unternehmen, die mit 30.000 bis 40.000 Mitarbeitern in die Cloud gewandert sind." Ich beglückwünsche den Kollegen zu Panasonic. 300.000 Mitarbeiter, die nun Zugriff auf Cloud Computing-Lösungen haben, sind eine beeindruckende Zahl. Auch wir bei Google können einige sehr respektable große multinationale Konzerne als Kunden vorweisen, die auf Cloud Computing setzen. Je mehr Referenzkunden, umso eher kann ich Vertrauen aufbauen und stärken. Und das ist unser Job.

Prof. Picot:
Ich möchte gern Herrn Sirtl noch kurz das Wort geben, um seine Sicht auf diese Fragen zu geben und dann zum Abschluss unsere drei Kundenvertreter bitten, in zwei, drei Punkten zu sagen, was sie gelernt haben und was sich für sie verändert hat.

Herr Sirtl:
Die Frage, wem eigentlich die Provider vertrauen, ist eine sehr interessante Frage. Wenn Sie sich die Vertreter, die hier oben sitzen, anschauen, wird jeder sagen, dass sie so gut wie alles selber machen. Ein Kollege von Google hat gesagt: wir bauen die Server selber und deswegen kann er auch so selbstbewusst da sitzen und sagen, dass er in die eigene Leistung vertraut. Genauso machen wir es. Tatsächlich behalten wir relativ viel unter unserer Kontrolle, weil wir auch da uns selbst am meisten vertrauen. Deswegen machen wir Vieles selber. Zu den Fragen, ob die konfuse oder durchsichtige Wolke die bessere ist, bin ich der Verfechter der Theorie, dass die Hybridlösungen die Zukunft sein werden. Wir wollen den Kunden die Wahlfreiheit geben, wie diffus es sein soll und wie transparent es sein kann, indem er wählen kann, wie viele Vorgaben er in seiner IT Lösung vorgegeben haben möchte oder wie viel er generisch zukauft. Ein Konzept, was leider ein bisschen untergegangen ist, was ich aber sehr schön fand von Herrn Dr. Unkel, ist das Thema

Serviceorientierung, das meiner Meinung auch Schlüssel für diese ganze Diskussion ist. Serviceorientierung in Reinform würde heißen, dass mich nur die Schnittstelle interessiert und Service Level vielleicht, aber die interne Funktionsweise ist mir egal. Dann habe ich wirklich das Cloud Computing in Reinform und überlasse dem Provider alles, was für die Bereitstellung dieses Service notwendig ist und vertraue ihm. Wenn ich dieses Vertrauen nicht entgegenbringe und intern doch ein paar Stellschrauben drehen möchte. So ist es beispielsweise in unserer Plattform möglich – dass ich sagen kann; dass ich hier Stellschrauben drehen oder auch alles selber machen kann auf unserer Plattform. Nur verzichte ich dann darauf, von den Skaleneffekten, die sich durch diese völlige Flexibilität ergeben, zu profitieren. Von daher die Antwort auf Ihre Frage. Wenn die Incentives hoch genug sind, gehe ich in die Cloud. Ich würde sagen, der Kunde wählt quasi flexibel, wo er seine Daten haben will, in der Cloud, bei einem Hoster usw. und kann sich für eines dieser Modelle entscheiden anhand der Vorteile, die sich ihm bieten, vielleicht Kostenersparnis, aber auch anhand der möglichen Risiken, die er selber einschätzen muss und die Frage, ob er bereit ist, diese einzugehen oder über Versicherungen absichern kann. Das heißt, er kann sich möglicherweise in die Cloud begeben oder das Ganze Vorort machen. Von daher sage ich, dass in der Zukunft sicher die Hybridlösungen das sein werden, wo es hingeht.

Prof. Picot:
Vielen Dank, Herr Sirtl. Jetzt kommt die Schlussrunde unserer drei Kundenvertreter. Ich beginne bei Herrn Dr. Unkel an. Ganz kurz: Was haben Sie gelernt, was Ihren Blick auf die Cloud und das, was damit zusammenhängt für Ihre Zukunft verändert und vielleicht auch anders einschätzen lässt als Sie es ursprünglich getan haben heute?

Dr. Unkel:
Ich sehe zunächst einmal keinen Ansatzpunkt meine Aussagen, die ich soeben und heute Morgen getroffen habe, zu verändern. Im Gegenteil sehe ich mich hier sehr schön bestätigt. Die Mehrzahl der Vorträge hat eine nahezu gleichlautende Position vertreten. In dieser Podiumsdiskussion lag der Schwerpunkt der Diskussion eher beim Cloud Einsatz im Endanwenderumfeld. Bei großen Unternehmen liegt ein anderes Einsatzumfeld vor, das insbesondere auf IT Anwendungen in speziellen Kernprozessen ausgerichtet ist. Hierauf hat Herr Dr. Götz mit seinem Diskussionsbeitrag auch soeben hingewiesen.

Es freut mich von den Diskussionsteilnehmern der IT Providerseite zu hören, dass sie keine schlagartige Verbreitung von Cloud Computing wie bei einem „Big Bang“ erwarten, sondern eher eine evolutionäre Entwicklung sehen. Das entspricht auch unserer Erwartung. Evolutionär heißt, und da sind wir wieder beim Thema Vertrauen, Stück für Stück Erkenntnisse gewinnen, Versuche unternehmen, Erfahrungen sammeln und so Vertrauen aufbauen. Daneben werden wir, wie gesagt, auf

den Aspekt der Nachhaltigkeit bei der Marktverbreitung von Cloud Computing achten.

Dr. Räther:
Der Ansatz, das Vertrauen der Kunden gewinnen zu wollen, spielt natürlich im Banking auch eine große Rolle. Wir haben allerdings noch einen anderen großen Player. Das ist der Staat, als Regulator und Gesetzgeber. Wenn Sie heute einer BaFin sagen, dass Sie nicht wissen, wo Ihre Daten sind, wird die Ihnen kaum folgen. Hier gibt es auch noch viel Überzeugungsarbeit zu leisten.

Den zweiten Punkt fand ich ganz interessant: dass Vertrauen durch Transparenz gewonnen werden kann. Herr Sirtl, Sie haben angeregt, dass man eben auch den Cloud Usern wirklich sagt, wo ihre Daten sind, um damit die Geschäftsprozesse transparenter zu machen. Dann kann der Konsument aber auch der Regulator Vertrauen finden und vielleicht auch Clouds akzeptieren.

Herr Leistenschneider:
Für mich war die gesamte Veranstaltung eine Bestätigung dafür, dass die DATEV bei diesem Thema auf dem richtigen Weg ist und dass der in der Vergangenheit eingeschlagene Weg ebenfalls der „richtige" war. Wir werden auch in Zukunft die Entwicklungen bei Cloud Computing genau beobachten. Dazu haben wir vor einem halben Jahr in unserem Haus ein eigenes Cloud Kompetenz-Center eingerichtet, was sich intensiv mit allen Fragen rund um die Cloud befasst.

Erwähnen möchte ich noch, dass gerade bei diesem Thema, nachhaltiges Handeln für DATEV eine große Rolle spielt. Bei der Genossenschaft steht die nachhaltige wirtschaftliche Förderung ihrer Mitglieder im Vordergrund und nicht der kurzfristige schnelle Erfolg, wie das bei kapitalistisch orientierten Unternehmen häufig der Fall ist. Das schafft Vertrauen und damit eine wichtige Voraussetzung für das Funktionieren einer erfolgreichen Private Cloud.

Auf einen weiteren Aspekt mochte ich noch eingehen. In einigen Beiträgen wurde die Meinung vertreten, dass sich der Gesetzgeber ändern müsse, um Fortschritte bei der Verbreitung von Cloud Computing zu erzielen. Als Beispiele wurden bestehende datenschutzrechtliche Bestimmungen insbesondere in der EU sowie die aktuelle Steuergesetzgebung genannt. Gerade beim letztgenannten Thema bin ich der Meinung, dass dies nicht so schnell passieren wird. Der Steuergesetzgeber hat immer die Sicherung des Steueraufkommens im Auge. Gerade beim Umsatzsteuerbetrug – Stichwort „Karussellgeschäfte" – wird der Fiskus kaum mit sich reden lassen. Diskussionen, wie sie jetzt beim Thema „Elektronische Rechnung" aufgekommen sind zeigen deutlich, dass der Steuergesetzgeber an einem hohen Sicherheitsniveau, wie es z.B. qualifizierte elektronische Signaturen bieten, festhält. Ähnlich wird er sich beim Thema Datenzugriff verhalten. Zur Sicherung des Steueraufkommens und zur problemlosen Prüfbarkeit steuerrelevanter Daten werden die Finanzbehörden auch künftig darauf bestehen, dass solche Daten physisch auf Servern im Erhebungsge-

biet bzw. mit entsprechenden Auflagen innerhalb der EU den Steuerprüfern für einen uneingeschränkten Datenzugriff zur Verfügung stehen. Deswegen glaube ich nicht, dass sich im Hinblick auf die Möglichkeiten des Cloud Computing an der Steuergesetzgebung in diesem Punkt kurz- und mittelfristig viel verändern wird. Es wird wohl noch ein paar Jahre dauern, bis der Steuergesetzgeber einer Cloud das notwendige Vertrauen entgegenbringen wird.

Prof. Picot:
Ganz herzlichen Dank. Meine Damen und Herren, ich glaube, dieser Schlusspanel hat für sich schon die Funktion einer gewissen Zusammenfassung und Zusammenschau der verschiedenen Perspektiven Themenstränge gehabt. Ich werde nicht eine Zusammenfassung der Zusammenfassungen und der sonstigen Aspekte hier versuchen. Ich habe den Eindruck, dass wir mit einem Erkenntnisgewinn und einem geschärften Blick für die zukünftigen Entwicklungen aus dieser Konferenz herausgehen. Die Konferenz hat ein Thema angesprochen, das einen wirklichen Strukturwandel adressiert, der sich derzeit abspielt und der sich wohl noch erheblich verstärken wird. Ich möchte betonen, was auch zum Beispiel Herr Dueck und andere gesagt haben, dass Geschäftsmodelle, die selbstverständlich schienen, nicht mehr haltbar sind und neue Player und neue Dienstleister hervortreten, zum Teil in ganz anderer Formation und Marktstruktur als wir das bisher kannten. Diese Cloud Anbieter skalieren sehr stark und wir wissen, dass überall dort, wo Skalierung eine Rolle spielt, auch Konzentrationsbewegungen mit allen Vor- und Nachteilen entstehen können. Das ändert die Märkte. Aber es bietet auch neuartige Leistungen, Dienstleistungen, die wir in dieser Form und zu dieser Kostengünstigkeit und auch mit dieser Qualität bisher nicht kannten. Wir haben einen Blick auf eine im säkularen Zusammenhang sich rapide verändernde Welt geworfen, in der wir Vertrauen genauso nötig haben, wie wir es auch sonst immer nötig hatten und auch immer nötig haben werden in unserem gesellschaftlichen und wirtschaftlichen Leben. Denn, das ist uns auch heute klar geworden, wir können das erforderliche Vertrauen durch Kontrolle, Automation oder Zwang nicht völlig ersetzen. Das ist nicht möglich. Wir haben stets Lücken in unseren Kooperationsbeziehungen, die wir füllen müssen mit gewachsenem Vertrauen, das über die Zeit akkumuliert wird. Dieser Akkumulierungsprozess lässt sich nicht verordnen über Nacht, sondern ist ein Erfahrungsprozess, der sich über die Zeit hinweg anhäuft.

Ich möchte mich bei allen bedanken, die mitgewirkt haben, bei allen aktiven Redner, zuletzt hier auf dem Podium, bei allen Diskutanten, aber auch bei Ihnen allen, die Sie der Konferenz Ihre Aufmerksamkeit geschenkt haben, vor allen Dingen aber auch Herrn Udo Hertz (IBM) und seinem Team, der diese Konferenz sorgfältig und langfristig vorbereitet hat, was nicht einfach war, weil diese Thematik nicht so einfach zu strukturieren war und dafür die entsprechenden Fachleute zu bekommen. Dafür ganz herzlichen Dank, aber auch dem Team vom Münchner Kreis, das diese Konferenz gut vorbereitet und organisatorisch durchgeführt hat.

Ich freue mich auf unsere nächste Zusammenkunft im Münchner Kreis. Sie haben die Vorankündigung vorliegen; 15./16. Juni über Next Generation Communication, ebenfalls ein außerordentlich spannendes und zukunftsweisendes Thema, auch mit vielen offenen Flanken, wie das bei interessanten Themen immer so ist und würde mich freuen, wenn wir jetzt noch den einen oder anderen Gedanken austauschen und draußen bei einem kleinen Empfang fortsetzen können. Ihnen auf jeden Fall ansonsten einen guten Heimweg und auf baldiges Wiedersehen. Nochmals vielen Dank hier auf dem Podium.

Anhang

Liste der Referenten und Moderatoren

Michael Auerbach

T-Systems International GmbH
Ltr. SDM
Heinrich-Hertz-Str. 1
64295 Darmstadt
michael.auerbach@t-systems.com

Uwe Bernd-Striebeck

Partner
KPMG AG
Wirtschaftsprüfungsgesellschaft
Alfredstr. 277
45133 Essen
uberndstriebeck@kpmg.com

Prof. Dr. Gunter Dueck

Chief Technologist
IBM Deutschland GmbH
Gottlieb-Daimler-Str. 12
68165 Mannheim
dueck@de.ibm.com

Dr. Alexander Duisberg

Partner
Bird & Bird LLP
Pacellistr. 14
80333 München
alexander.duisberg@twobirds.com

Kai Gutzeit

Head of Enterprise, DACH & Nordics
Google Enterprise EMEA
Google Germany GmbH
Dienerstr. 12
80331 München
kgutzeit@google.com

Dr. Thomas Götz

Managing Partner
Detecon International GmbH
Oberkasseler Str. 2
53227 Bonn
thomas.goetz@detecon.com

Udo Hertz

Director of Information Management Development
IBM Deutschland Research & Development GmbH
Schönaicher Str. 220
71032 Böblingen
udo.hertz@de.ibm.com

Michael Leistenschneider

Vorstandsmitglied
DATEV eG
90329 Nürnberg
michael.leistenschneider@datev.de

Dr. Guido Möllering

Max-Planck-Institut für Gesellschaftsforschung
Paulstr. 3
50676 Köln
gm@mpifg.de

Prof. Dr. Günter Müller

Universität Freiburg
IS für Informatik u. Gesellschaft,
Abt. Telematik
Friedrichstr. 50
79098 Freiburg
mueller@iig.uni-freiburg.de

A. Picot et al. (eds.), *Trust in IT*, DOI 10.1007/978-3-642-18110-8,

Prof. Dr. Dres. h.c. Arnold Picot

Ludwig-Maximilians-Universität
München
IS für Information, Organisation und
Management
Ludwigstr. 28
80539 München
picot@lmu.de

Dr. Philipp Räther

UBS Investment Bank
Legal & Compliance –
Office of the COO
3 Finsbury Avenue
London EC2M 2PA, UK
Philipp.Raether@ubs.com

MinDir Martin Schallbruch

Bundesministerium des Innern
IT-Direktor und Chief Information
Officer
Alt-Moabit 101 d
10559 Berlin
Martin.Schallbruch@bmi.bund.de

Andreas Schlayer

Topic Network Leader
Münchener Rückversicherungs-
Gesellschaft AG
Königinstr. 107
80802 München
aschlayer@munichre.com

Prof. Dr. Jörg Schwenk

Ruhr-Universität Bochum
Lehrstuhl für Netz- und Datensicherheit
Universitätsstr. 150
44780 Bochum
joerg.schwenk@rub.de

Holger Sirtl

Microsoft Deutschland GmbH
Deveöpüer Üöatfpr, & Strategy Group
Konrad-Zuse-Str. 1
85716 Unterschleißheim
hsirtl@microsoft.com

Dr. Peter Unkel

RWE Power Aktiengesellschaft
Unternehmensentwicklung
Informationsmanagement
Huyssenallee 2
45128 Essen
Peter.Unkel@rwe.com

Klaus-Dieter Wolfenstetter

Deutsche Telekom AG, Laboratories
Innovation Development
Ernst-Reuter-Platz 7
10587 Berlin
k.wolfenstetter@telekom.de