HZD
Hessische Zentrale für Datenverarbeitung

HESSEN

Trendbericht 2012


Architektur


Internet


Technik


IT-Sicherheit


Cloud Computing


Web-Office


Tablets

Kleptografie

USDL


FTTx

LTE

Trendbericht

Inhalt

Vorwort 4

Zu diesem Text 5

Verwaltungsrelevanz 5
Marktreife/Produktverfügbarkeit 5
Umsetzungsgeschwindigkeit 5

Architektur & Prozesse 6

„Bring your own Device“ 6
USDL – Standardbeschreibungen für Dienste? 9

Trend-Spezial 11

Heiter bis wolkig – Cloud Computing 11

Anwendungen & Web 19

Die Welt ist mein Büro – Web-Office 19
Social Media als Mail-Ersatz? 20
Anwendungen? Da gibt’s doch was vom App-Store! 23
Mobiles Bezahlen mit dem Handy 25

Technik 27

Auf dem silbernen Tablet 27
Graphén – der Stoff, aus dem die Träume sind 28
BIOS ade? Jetzt kommt UEFI! 29
LTE – Long Term Evolution 31
Höher, schneller, weiter – Wi-Fi entwickelt sich 33
FTTx – Glasfaser überall 35
Licht aus – Spot an zur Datenübertragung 37

IT-Sicherheit 39

Ich weiß, was du letzte Woche gelesen hast! – History Stealing 39
Mit den eigenen Waffen – Kryptovirologie und Kleptografie 41
Secure by design – für die innere Sicherheit 43

Vorwort

Informations- und Kommunikationstechnik findet man heute überall. Das ist nichts Neues. Computer stehen schon lange in vielen Firmen und Wohnungen. Handys sind längst nicht mehr das Privileg von Geschäftsreisenden, sondern begegnen uns – aufgerüstet zu mobilen Minibüros mit eingebauter Spielkonsole, Videothek und Internetzugang – täglich in Bus und Bahn, in Geschäften oder auf dem Schulhof. Was allerdings neu ist, ist die Tatsache, dass Geräte und Anwendungen, die zunächst für den privaten Gebrauch bestimmt sind, die Entwicklung der IT deutlich prägen, wenn nicht gar bestimmen. Soziale Netzwerke, Tablet-Computer und „Apps“ kommen zuerst im Privatbereich zum Einsatz. Schnelle Netzzugänge abseits der Wirtschaftszentren sind für Videostreaming zuhause mindestens so interessant wie für Fachanwendungen ortsansässiger Unternehmen. Mobiles Bezahlen mit dem Handy wendet sich auch eher an private Konsumenten, die unterwegs kleine und mittlere Beträge begleichen wollen, als dass große Transaktionen im Wirtschaftsleben darüber abgewickelt werden sollen. Viele dieser IT-Entwicklungen im Privatbereich sind innovativ und haben das Potenzial, auch in Unternehmen und Organisationen die Arbeit zu unterstützen. Daher wundert es nicht, dass man immer wieder Überlegungen dazu findet, wie so etwas konkret umgesetzt werden kann. Dies reicht bis zu Konzepten, die Privat-IT in Unternehmen zu integrieren: „Bring your own Device!“

All diese Anwendungsfälle im Alltag setzen komplexe Infrastrukturen voraus. Nicht nur die Basistechnik und „smarte“ Endgeräte müssen überall verfügbar sein, sondern auch Dienste und Anwendungen. Das Vehikel dafür ist Cloud Computing. Doch was für private Daten handhabbar und unkritisch sein mag, muss erst noch seine Eignung für den Einsatz in Bereichen mit erhöhten Sicherheitsanforderungen wie Unternehmen und Verwaltungen nachweisen. Vor diesem Hintergrund entwickeln sich die hier vorgestellten Trends weiter. Es wird spannend sein, ihre Bedeutung für die öffentlichen Verwaltungen weiterzuverfolgen.

Zu diesem Trendbericht haben zahlreiche Kolleginnen und Kollegen ihr Fachwissen beigesteuert. Ein besonderer Dank für die Unterstützung geht an Ralf Baecker, Dr. Miriam Büßelberg, Dr. Arno Domack, Lukas Heuser, Dr. Stefan Kahlert, Horst Kiehl, Christoph Leistner, Peter Müller, Dr. Klaus-Dieter Niebling und Ingo Schwarz sowie an Dr. Daniel Oberle vom Forschungsprogramm Theseus zum Thema USDL.

Allen Leserinnen und Lesern wünschen wir eine interessante Lektüre.

Zu diesem Text

Mit dem Trendbericht ermöglichen wir unseren Leserinnen und Lesern einen Ausblick auf die aktuellen Trends in der Informationstechnologie. Dabei wollen wir uns jedoch nicht auf eine rein fachliche Information über die technischen Hintergründe und die weitere Entwicklung beschränken. Als IT-Gesamtdienstleister für die Hessische Landesverwaltung steht für uns die strategische Bedeutung der erfassten Trends für die Verwaltung im Mittelpunkt. Daher haben wir jedes einzelne Thema im Hinblick auf seine Auswirkungen auf die Verwaltung bewertet. Der Fokus liegt dabei auf der Hessischen Landesverwaltung. Neben einem kurzen Bewertungstext werden jeweils drei Kennzahlen angegeben, die die Einordnung der Themen in IT-strategische Überlegungen erlauben:

Verwaltungsrelevanz

Die Verwaltungsrelevanz gibt an, in welchem Maß ein Trend Auswirkungen auf die Verwaltung haben kann. Dies kann auf zweierlei Arten erfolgen: Zum einen können Trends zu technischen Änderungen in der IT-Landschaft führen bzw. diese ermöglichen. Sie sind daher in dem Maß verwaltungsrelevant, wie sie sich auf einige oder alle IT-Arbeitsplätze im Land auswirken. Dies kann den einzelnen Arbeitsplatz oder die Gesamtinfrastruktur betreffen.

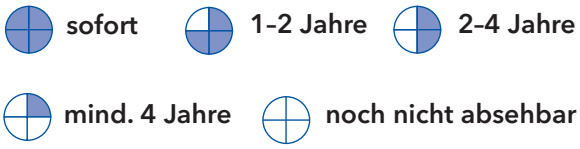
Zum anderen können IT-Trends dazu führen, dass sich Verwaltungsabläufe ändern oder ganz neue Abläufe etabliert werden (können). In diesen Fällen haben die IT-Trends also Auswirkungen auf die Kernprozesse der Verwaltung.

Die Verwaltungsrelevanz wird auf einer fünfteiligen Skala angegeben, die die Auswirkung des Trends auf die Verwaltung bewertet:

Auswirkung:

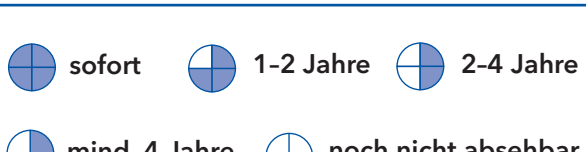
Marktreife/Produktverfügbarkeit

Der Wert für Marktreife bzw. Produktverfügbarkeit gibt an, wie lange es dauern wird, bis Produkte am Markt verfügbar sind, die auf der im Trend beschriebenen Entwicklung basieren. Die fünfteilige Skala gibt die Marktreife bzw. Produktverfügbarkeit mit folgenden Werten an:



Umsetzungsgeschwindigkeit

Die Umsetzungsgeschwindigkeit gibt an, wie schnell ein Trend in der Verwaltung umgesetzt werden kann. Sie kann als ein Maß für die Komplexität der entsprechenden Trendergebnisse gesehen werden: Je komplizierter ein Resultat oder Produkt ist, desto länger dauert es, dies in Verwaltung und Unternehmen nutzbar zu machen. Die fünfteilige Skala gibt die Einführungsgeschwindigkeit mit folgenden Werten an:



Architektur & Prozesse

„Bring your own Device"

Wer sich öfter auf Dienstreisen begibt, wird früher oder später auch mal mit der Frage konfrontiert, ob er einen Dienstwagen benutzen soll. Das sind dann in der Regel ganz passable Autos, mit denen man ordentlich fahren kann. Trotzdem muss man sich mal zunächst an das Fahrzeug gewöhnen – Wo war nochmal der Rückwärtsgang? –, das Navigationssystem lässt man lieber aus, bevor man 200 Seiten Bedienungsanleitung liest, und schließlich vermisst man während der Fahrt seine Lieblings-CD. Mancher wird es daher doch bevorzugen, statt des Dienstwagens sein Privatauto zu nutzen.

Wenn man einigen IT-Propheten glauben darf, bevorzugen auch IT-Anwender zunehmend ihre eigenen Geräte bei der Arbeit, und die Nutzung eigener „Betriebsmittel" am Arbeitsplatz ist ein ganz großer IT-Trend. Unter dem Motto „Bring your own Device" (ByoD) – engl. für „Bring dein eigenes Gerät mit" – propagieren sie eine IT-Strategie, bei der die Mitarbeiter von Firmen ihre privaten Geräte mit ins Unternehmen bringen und für die tägliche Arbeit nutzen. Das treibende Moment dabei ist aber nicht etwa ein entsprechender strategischer Ansatz, sondern vielmehr die Reaktion auf eine Änderung im Verhältnis der Mitarbeiter zur IT. Der Einstieg in die Thematik wird zumeist damit begründet, dass die Mitarbeiter das so wollten – und wenn sie es nicht dürften, es trotzdem machten. Also solle man lieber von vornherein einen entsprechend offenen Ansatz für den Einsatz privater Geräte wählen. Versüßt wird diese „Strategie" dadurch, dass reduzierte Administrationsaufwände in Aussicht gestellt werden, da die Mitarbeiter ihre eigenen Geräte ja kennen und entsprechend pflegen würden.

An dieser Stelle hat der Sicherheitsbeauftragte schon tief durchatmen müssen und auch vor manch einem Mitarbeiter mit starkem Bezug zur IT türmen sich die Fragen auf:

- Wie wird bei ByoD konkret ein definiertes Sicherheitsniveau erreicht bzw. sichergestellt?
- Wie werden dienstliche und private Daten getrennt?
- Wie steht es mit dem Datenschutz?
- Wer stellt sicher, dass spezifische dienstliche Anwendungen auf den privaten Geräten einwandfrei funktionieren?
- Was geschieht mit dienstlichen Daten, wenn das Gerät verloren geht?
- Wer ist für die Einhaltung von Arbeitsschutzbestimmungen zuständig?
- Wie wird eine evtl. gezahlte Nutzungsvergütung steuerlich behandelt?
- Wie werden Privatgeräte, die dienstlich genutzt werden, versichert?
- Wie kann bei der überwältigenden Vielzahl an Endgeräten und Betriebssystemversionen auf diesen Endgeräten ein adäquater Benutzersupport für dienstliche Funktionalitäten geleistet werden?
- Wie kann bei einem Privatgerät die Nutzung dienstlicher Anwendungen oder die Kenntnisnahme von dienstlichen Daten durch Dritte ausgeschlossen werden?

Obwohl diese Fragen nur an der Oberfläche mancher Themen kratzen, zeigen sie, dass der Einsatz beliebiger Privatgeräte im Arbeitsalltag ein sehr komplexes Unterfangen ist – insbesondere im Hinblick auf die IT-Sicherheit. So ist es nicht erstaunlich, dass in Umfragen zum Thema ByoD immer wieder die Bedrohung der Sicherheit als der kritischste Punkt gesehen wird. Dies gilt umso mehr bei Geräten, die nicht einmal über eine lokale Zugriffskontrolle verfügen.

Wenn es eingangs hieß, dass Mitarbeiter „sowieso" ihre Geräte einsetzen würden, gibt das einen Hinweis darauf, dass es mit Regelungen und Maßnahmen zu IT-Sicherheit in Unternehmen, die ByoD derart propagieren, nicht so weit her sein kann. Ansonsten wäre die willkürliche Einbindung fremder Geräte in die Unternehmens-IT nicht so ohne Weiteres möglich.

Wer sich auf das Abenteuer ByoD einlässt, muss also zunächst einmal

- die Auswirkungen auf die vorhandene und eine ggf. geplante IT-Architektur sowie auf bestehende Sicherheitskonzepte analysieren,
- Sicherheitsregeln für fremde Geräte sowie deren Zugriffsmöglichkeiten auf Daten definieren und
- Maßnahmen zentral gesteuert umsetzen, die die Einhaltung dieser Regeln gewährleisten.

Bei alledem muss gewährleistet sein, dass die für ByoD vereinbarten Spielregeln auch tatsächlich eingehalten werden. Da sich weder alles technisch erzwingen noch ausschließlich organisatorisch regeln lässt, müssen technische Maßnahmen und organisatorische Regelungen angemessen aufeinander abgestimmt werden. Durch die Konzeption und die Umsetzung solcher Regeln entstehen zusätzliche Aufwände, bevor Administrationsaufwände für Endgeräte eingespart werden können. Ob letzteres sich tatsächlich realisieren lässt, scheint auch fraglich, denn neben der Bereitstellung von Unternehmensanwendungen und Daten auf weitgehend standardisierten Geräten müssen nun noch die spezifischen Anpassungen für einzelne Geräte vorgenommen werden. Selbst wenn dies nicht im Rahmen interner Leistungen explizit kostenwirksam wird, entstehen ggf. implizit Kosten auf Seite der Mitarbeiter. Und wer ist für das Gerät zuständig, wenn sich beispielsweise die private Videoschnittsoftware und die betriebliche Fachanwendung nicht vertragen? Entsprechend gibt es Schätzungen, dass sich Administrationsaufwände durch ByoD verdoppeln.

So global und einfach, wie es in manchen Veröffentlichungen anklingt, scheint der ByoD-Ansatz also nicht zu sein und ist zumindest für den sporadischen Einsatz im Büroalltag nur wenig geeignet. Es lohnt sich aber trotzdem, die Frage zu stellen, in welchen Einsatzszenarien eigene Geräte die Unternehmens-IT sinnvoll ergänzen können und in welchen nicht:

Wer seine Arbeit am Computer täglich an einem festen Arbeitsplatz mit einer beschränkten Auswahl von Programmen verrichtet, wird zwar vielleicht seinen Social-Media-Client und sein komfortables Grafikprogramm vermissen, kann aber seine Aufgaben mit einem Standardarbeitsplatzrechner seines Arbeitgebers problemlos erledigen.

Wenn die Arbeit aber räumlich, zeitlich und inhaltlich flexibler wird, und die Grenzen zwischen Arbeit und Privatem nicht mehr scharf gezogen werden können – „hier Büro – da Zuhause“ –, entsteht auch schnell der Wunsch nach flexibler Technik. Wer auch außerhalb seiner Bürostunden einmal private und dienstliche Termine koordinieren muss, ist froh, wenn er den dienstlichen Terminkalender mit nach Hause nehmen kann. Und wer häufig außerhalb des eigenen Unternehmens arbeitet oder auf Dienstreisen ist, freut sich, wenn er für dienstliche Software und für private Anwendungen – z. B. Soziale Medien, private E-Mail oder eine kleine Musik- und Filmsammlung – nicht verschiedene Geräte herumtragen muss. Für den sporadischen Zugriff auf dienstliche Mail, auf Terminkalender und einfache Informationsdienste können ggf. Smartphones oder die modernen Tablet-Computer (➔ „Auf dem silbernen Tablet“) geeignet sein. Einen vollwertigen Arbeitsplatzrechner oder ein Notebook, auf dem Fachanwendungen laufen, können sie aber in der Regel nicht ersetzen und stellen somit zusätzliche Geräte dar. Ihre Einbindung als Privatgerät in die Unternehmens-IT bereitet also ggf. zusätzliche Aufwände, ohne Administrationskosten zu sparen.

Diese grob skizzierten Szenarien machen deutlich, dass der Umfang, in dem private und dienstliche Komponenten ggf. integriert werden müssen, sehr unterschiedlich sein kann.

Mitarbeiter, die mobil mit einem vernünftig ausgerüsteten Notebook arbeiten, können heute in der Regel über abgesicherte VPN-Verbindungen auf ihr Firmennetz zugreifen. Wenn dabei noch ein virtueller Desktop oder Webanwendungen benutzt werden, ist es fast egal, ob die Arbeit auf einem firmeneigenen oder auf einem privaten Gerät erledigt wird, sofern die grundlegenden Sicherheitsvorkehrungen getroffen und die o. g. Fragen geklärt werden. Dann müssen Arbeits- und Privat-„Welt“ auf dem Rechner hinreichend sauber getrennt sein. Sofern sich diese

Maßnahmen auf den infrage kommenden Endgeräten überhaupt umsetzen lassen, gelten sie aber nicht als besonders „smart“, da sie zusätzliche Authentisierungen u. ä. verlangen und somit gerade nicht den einheitlichen Zugriff auf Daten wie Telefonbuch, Adressen, Kalender oder E-Mail unterstützen. In der Folge haben es sog. Sandbox-Lösungen, die einen besonders gesicherten Bereich auf einem ansonsten mehr oder weniger offenen Gerät schaffen, schwer, sich am Markt zu behaupten.

Bei der Frage, ob „Bring your own Device“ die grundlegende IT-Strategie sein sollte, spielen also eine ganze Reihe von bestehenden Rahmenbedingungen eine wichtige Rolle. Dies sind der Grad an Standardisierung bzw. der Flexibilität der Arbeit hinsichtlich Ort, Zeit und Inhalt, die „Administratorfähigkeiten“ der Mitarbeiter, die bestehende oder geplante IT-Sicherheitsarchitektur oder die sowieso vorhandene Vielfalt an Endgeräten. Daneben haben auch mögliche Zielarchitekturen Einfluss auf die Umsetzung von ByoD: Sollen nur spezifische Geräte – oder Geräteklassen – auf bestimmte Anwendungen zugreifen können, oder sollen alle Anwendungen und Dienste offen für alle Geräte sein? Je offener die ByoD-Strategie ausgelegt ist, desto häufiger dürfte es erforderlich sein, Sicherheitsaspekte für Einzelfälle zu betrachten und Speziallösungen zu erarbeiten. Ansonsten scheint es naheliegend, bei der Öffnung der Unternehmens-IT nach Geräteklassen – Smartphone, Tablet, Notebook, sonst. Rechner – und benötigten Daten bzw. Anwendungen und Diensten zu unterscheiden.

Auch in Unternehmen und Organisationen, in denen die Arbeitsstrukturen relativ standardisiert sind und zunächst kein Bedarf an einer durchgängigen „Bring your own Device“-Strategie besteht, lohnt es sich evtl., sich mit den Auswirkungen von Privatgeräten in der Unternehmens-IT zu befassen. Das kann wertvolle Hinweise darauf geben, wie die IT-Landschaft zugleich flexibel und doch sicher gestaltet werden kann. Und das zahlt sich evtl. aus, wenn die „Standard-IT“ an manchen Stellen verändert werden muss – oder der neue Chef doch sein neues Lieblingsgerät mitbringt.

Bewertung

Die Informations- und Kommunikationstechnik an Verwaltungsarbeitsplätzen ist i. d. R. in weiten Bereichen stark standardisiert. Daher schiene hier auf den ersten Blick ein „Bring your own Device“-Ansatz mehr dem Spieltrieb Einzelner geschuldet, als dass er eine umfassende Strategie darstellen würde. Trotzdem – oder gerade wegen der hohen Standardisierung der normalen Arbeitsplätze – gibt es einige Bereiche, in denen es durchaus lohnt, das Konzept und seine Auswirkungen zu bedenken: Für alle Verwaltungsmitarbeiter, die unter wechselnden Rahmenbedingungen – örtlich, zeitlich, fachlich oder technisch – arbeiten, ist es ggf. sinnvoll und hilfreich, eigene Geräte einsetzen zu können. Dies könnten einerseits private Geräte oder aber Geräte aus einem anderen Zuständigkeitsbereich der Verwaltung sein. Auch bei externen Mitarbeitern kann es sinnvoll sein, wenn diese ihre eigenen Werkzeuge mitbringen können. In allen diesen Fällen müssen die Rahmenbedingungen für einen solchen Einsatz und die technischen Lösungen vorab definiert sein. ByoD wird gerade erst in Unternehmen und Organisationen erprobt. Die dort gesammelten Erfahrungen mit Konzepten und technischen Lösungen für das IT-Management privater Komponenten sowie zu den finanziellen Auswirkungen von „Bring your own Device“ könnten auch für Verwaltungen wertvolle Hinweise für eigene Ansätze liefern. Auf jeden Fall sollte der Zugang zu der Thematik strategisch und nicht als Reaktion auf den Markt erfolgen.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit*:	

** Derzeit ist noch nicht absehbar, wann es Produkte geben wird, die eine universelle ByoD-Strategie umfassend unterstützen werden. Es gibt allerdings bereits eine Reihe von Werkzeugen und Lösungsmustern, die spezifische Szenarien unterstützen.*

USDL – Standardbeschreibungen für Dienste?

Im Zusammenhang mit der IT-Umsetzung der EU-Dienstleistungsrichtlinie (DLR) tauchte immer wieder das Schlagwort „Prozessketten“ auf, das deutlich machte, welche ehrgeizigen Ziele man in diesem Projekt verfolgen konnte. Das fachliche Ziel der DLR ist es, Hemmnisse für die grenzübergreifende Erbringung von wirtschaftlichen Dienstleistungen in der EU abzubauen. Zu den dafür relevanten Verfahren zählt in Deutschland z. B. die Anmeldung eines Gewerbes. Schnell wurde deutlich, dass es für die durchgängige IT-Unterstützung bei der Abwicklung solcher Verfahren nicht ausreicht, diese als jeweils einzelnen Prozess zu betrachten. Vielmehr können bei der Erfüllung komplexer Aufgaben ganze Prozessketten mit unterschiedlichen Zuständigkeiten und Beteiligten ablaufen – auch wenn diese für den Dienstleister als nur eine Maßnahme wahrgenommen werden (z. B. „Genehmigung von ...“). Die Modellierung solcher Prozessketten erwies sich jedoch schon auf fachlicher Ebene als sehr komplex.

Im Rahmen des deutschen Forschungsprogramms THESEUS wird eine Plattform, Texo, entwickelt, die es ermöglichen soll, Dienste im Internet wie Güter zu handeln und online miteinander zu kombinieren. Eine wesentliche Grundlage dafür ist die Spezifikationssprache USDL, Unified Service Description Language, mit deren Hilfe Dienste „für Maschine und Mensch interpretierbar gemacht werden“ sollen.

Um dies gewährleisten zu können, muss eine Spezifikationssprache vielen Anforderungen genügen. Sie muss auf der einen Seite sehr formal strukturiert und erweiterbar sein, sie soll Modularität unterstützen, um die Komplexität von Anwendungsgebieten in den Griff zu bekommen, und sie muss in dem Sinne Verständlichkeit unterstützen, dass sie z. B. die formale Verfeinerungen von Beschreibungen ermöglicht. Auf der anderen Seite müssen betrieblich-organisatorische Aspekte – wie z. B. Ressourcen oder fachliche Voraussetzungen – der zu beschreibenden Dienste in der Sprache darstellbar sein, ohne Details über die Ausführung des Dienstes zu verraten. Durch die starke Ausrichtung auf die Beschreibung von Wirtschaftsdiensten ist USDL eine für diese Anwendungsdomäne spezifische Sprache. Dies spiegelt sich auch in den Bezeichnungen und Inhalten der USDL-Module wider: So werden neben Modulen für die funktionale und die technische Beschreibung des Dienstes im Modul „Participants“ die an einem Service beteiligten Rollen beschrieben, „Pricing“ erfasst die Informationen zur Preisgestaltung, es gibt Module zu Service Levels oder rechtlichen Aspekten wie z. B. dem Copyright.

So lassen sich die einzelnen Schritte komplexer wirtschaftlicher Abläufe formal einheitlich beschreiben und nach außen hin in einen Prozessumschlag packen, der – ebenfalls formal beschrieben – den Ablauf repräsentiert. Liegen für mehrere konkrete Dienstleistungen solche formalen und maschinenlesbaren Beschreibungen vor, lassen sich die Suche nach einem solchen Dienst und dessen Buchung automatisieren. So könnte z. B. der Produzent einer Ware über das Internet Angebote für deren Lieferung an einen konkreten Ort einholen, vergleichen und ggf. buchen. Wie verschiedene Spediteure diesen Dienst erbringen, muss ihn dabei nicht interessieren, auch wenn der Ablauf selber wieder viele Teilprozesse erfordert – z. B. Einholen von Genehmigungen, Buchung verschiedener Transportmittel, Organisation und Durchführung des Transportes, Versicherungen etc. Durch die flächenhafte, formale Beschreibung von Prozessen mittels USDL ließe sich ein großer Schritt in Richtung eines „Internets der Dienste“ machen.

Schon aus dieser sehr groben Beschreibung der Anforderungen an eine Spezifikationssprache für Dienste und dem Beispiel wird aber deutlich, dass es sich dabei um ein komplexes Instrument handelt. Um die Anwendbarkeit des bisher entwickelten Modells zu verbessern und seine Akzeptanz zu fördern, wird für USDL die Standardisierung durch das World Wide Web Consortium, W3C, angestrebt.

Bewertung

Da es sich bei USDL um eine domänenspezifische Spezifikationssprache handelt, die für die Beschreibung von Wirtschaftsprozessen entwickelt wurde, wird sie nicht unmittelbar einen Beitrag zur eingangs beschriebenen Modellierung von Prozessketten in der Verwaltung leisten können. Nichtsdestoweniger könnte USDL als Vorlage für eine Spezifikation von Verwaltungsprozessen dienen, die sowohl von Menschen verstanden werden kann, als auch der Automation von entsprechenden Prozessketten dienen kann. Daneben ist der öffentliche Bereich sowohl Dienstleister für die Wirtschaft wie auch – in seiner Gesamtheit – einer der größten Einkäufer in Deutschland. Entsprechend dürften auch die wirtschaftsspezifischen Prozessbeschreibungen im Hinblick auf die – evtl. automatisierte – Beschaffung von Dienstleistungen und Gütern auch für Verwaltungen interessant sein, sofern sich diese am Markt etablieren. Daher ist es durchaus sinnvoll, das Thema USDL auch seitens der öffentlichen Verwaltungen weiterzuverfolgen.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Trend-Spezial

Heiter bis wolkig – Cloud Computing

Ein bedeckter Himmel mit geschlossener Wolkendecke drückt bei vielen Menschen die Stimmung. Sie hoffen eher auf blauen Himmel und Sonne. Doch dann wird es – zumindest im Sommer – schnell zu heiß und man sehnt sich nach einigen wenigen Wolken. Dieses Bild von zu viel bzw. zu wenig Wolken lässt sich ganz gut auf die Situation des Cloud Computing übertragen: Weder der Ansatz, alle Informationstechnik und -dienste in einer IT-Cloud zu verstecken, noch der traditionelle Weg, alles individuell zu betreiben, scheinen den Erwartungen und den Befürchtungen in Bezug auf Cloud Computing gerecht zu werden. Also ist einmal mehr der goldene Mittelweg gefragt.

Der Begriff „Cloud Computing“ bezeichnet hier die Bereitstellung von Informationstechnik und -diensten in einem großen Pool, bei deren Nutzung der Kunde nicht unbedingt weiß, welche konkreten Ressourcen dabei verwendet werden. Diese werden bedarfsgerecht eingesetzt und abgerechnet. Im HZD-Trendbericht für 2008/2009 hatten wir dies auf die einfache Formel „Cloud = Grid + SaaS“ gebracht. Dabei steht „Grid“ für die bereitgestellte vernetzte Infrastruktur – also das technische Rückgrat der Wolke. „SaaS“, die Abkürzung für „Software as a Service“, steht für die Bereitstellung maßgeschneiderter Dienste aus der Wolke.

Auch vielen Befürwortern möglichst umfangreicher und universeller Cloud-Architekturen ist klar, dass gerade im Bereich der öffentlichen Verwaltung Rahmenbedingungen für den IT-Betrieb existieren, die die vollständige Verlagerung von Verwaltungs-IT in öffentlich am Markt angebotene Clouds nicht oder nur bedingt möglich machen. Da sind zum einen die großen und spezifischen Bestände an Anwendungen und Daten. Um diese auf eine Cloud-Plattform zu verlagern, müssten sie in hohem Maße virtualisierbar und standardisierbar sein. Nur dann kann die dynamische Verwaltung von Ressourcen in einer Cloud vorteilhaft genutzt werden. Dazu kommt eine Reihe von rechtlichen und organisatorischen Rahmenbedingungen, die die Verarbeitung von Daten auf solchen Maschinen erschweren, die nicht der Kontrolle der Verwaltung unterliegen. Dies sind z. B. datenschutzrechtliche Vorgaben. Hier bietet die sog. Auftragsdatenverarbeitung ggf. einen Ausweg. Auftragsdatenverarbeitung findet dann statt, wenn die Datenverarbeitung von Dritten durchgeführt wird, die Verantwortung für die ordnungsgemäße Durchführung aber weiterhin beim Auftraggeber verbleibt.

Dazu müssen zahlreiche Details genau geregelt und schriftlich vereinbart werden – so z. B. die eingesetzten Programme oder Maßnahmen zu Datenschutz und Datensicherheit. Es obliegt auch dem Auftraggeber, die Einhaltung dieser Vereinbarungen zu überprüfen. Obwohl diese Auftragsdatenverarbeitung im gesamten Europäischen Wirtschaftsraum möglich ist, laufen die strengen Regeln doch der Idee eines relativ ungebundenen IT-Betriebs in der Cloud zuwider. Schon die spezifische Vereinbarung detaillierter Servicelevel und weiterer organisatorischer und ggf. technischer Details entspricht nicht der Vorstellung vom unkomplizierten Bezug von Rechen- oder Dienstleistung „aus der Steckdose“.

Im Folgenden werden einige Aspekte von Cloud Computing tiefer gehend betrachtet, die insbesondere für die öffentliche Verwaltung von Bedeutung sind. Dazu werden zunächst einige Begriffe erläutert, die der Charakterisierung verschiedener Cloud-Modelle dienen und die sich inzwischen etabliert haben.

Charakterisierung

public – private – hybrid – community – personal

Das einfachste Bild von Cloud Computing besteht aus nur einer Wolke, aus der alle Leistungen kommen. Der Zugriff erfolgt über das Internet, so dass „alles überall“ zu haben ist. Da verschiedene Provider ihre Leistungen aber separat verkaufen wollen, ist der IT-Himmel eher mit einer großen Menge an verschiedenen Wölkchen übersät. Trotzdem stehen die Leistungen über öffentliche Netze allen potenziellen Nutzern offen. In diesem Fall spricht man von „öffentlichen“ bzw. „Public Clouds“. Diese skalieren gut über die Zahl der Nutzer von Diensten, die

weitgehend standardisiert sind, und den Umfang der Nutzung (z. B. Rechenleistung oder Speicherplatz).

Was zunächst sehr einfach und komfortabel wirkt, wirft bei näherem Hinsehen aber auch eine Reihe von Fragen auf. Einer der Hauptkritikpunkte an Public Clouds bezieht sich auf den Schutz der eigenen Daten in der Wolke. Der Grundgedanke von Cloud Computing besteht ja darin, einem Anwender gerade keine dedizierten Ressourcen zur Verfügung zu stellen. Es gibt also zunächst keine Garantie, dass bestimmte Maschinen exklusiv genutzt werden, noch kann genau festgelegt werden, welche Maschinen zum Einsatz kommen. Auch Anwendungen und Dienste wie z. B. Datenbanken oder Webserver stehen ggf. mehreren Nutzern zur Verfügung. Es kann also durchaus sein, dass die Daten einer Firma auf den gleichen Systemen verarbeitet werden wie die des Konkurrenten. Das legt zum einen nahe, starke Sicherheitsmaßnahmen zum Schutz und zur Abgrenzung der Daten zu ergreifen. Das hat zum anderen aber auch zu einem Cloud-Modell geführt, das die vollständige Kontrolle über Hard- und Software beim Kunden belässt – der sog. Private Cloud. Unabhängig davon, ob diese vom Kunden selbst oder von einem externen Provider betrieben wird, stehen die Hardware- und Softwarekomponenten ausschließlich ihm zur Verfügung. Auch Datenbanken und andere Dienste werden ggf. exklusiv betrieben. Hier wird schnell klar, dass die Skalierung über viele Anwender gegenüber dem „unendlich“ erscheinenden Potenzial bei der Public Cloud stark eingeschränkt ist. Die Private Cloud skaliert daher stärker über die Zahl der Dienste, die auf der exklusiven Hardware angeboten werden kann.

Neben der Frage, ob ein in die Cloud ausgelagerter IT-Betrieb die Kosten senken kann, ist die Frage der Dimensionierung von IT-Landschaften ein wichtiger Treiber für Cloud-Anwendungen. Bei exklusiven Ressourcen müssen die Systeme immer für die mögliche Spitzenlast ausgelegt sein – auch wenn diese nur selten erreicht wird. Die über die „Menge“ einer Dienstleistung skalierende Cloud kann solche Spitzenlasten einfach und damit kostengünstig abfedern. In der Folge erscheint es logisch, für Anwendungen, die solche Spitzenlastprobleme mit sich bringen, die Private Cloud um Dienste aus einer Public Cloud zu ergänzen: Wenn die internen Kapazitäten für einen überschaubaren Zeitraum überlastet werden, werden öffentlich zugänglich Ressourcen aus einer Public Cloud zugeschaltet. Allerdings stellen sich auch hier wieder die o. g. Sicherheitsfragen – wenn auch nur für einen beschränkten Zeitraum. Eine solche Kombination von Private und Public Cloud nennt man auch Hybrid Cloud.

Ein weiteres Modell, um die Beschränkung von Ressourcen vorübergehend abfangen zu können, ohne dabei einen geschützten Bereich zu verlassen, ist die sog. Community Cloud. Diese wird von verschiedenen, sich einander vertrauenden Organisationen nach gemeinsamen Regeln betrieben, wobei jeder Partner die Infrastruktur- und Dienstleistungen seiner Private Cloud in einem gewissen Umfang einbringt. Hierdurch lassen sich maßgeschneiderte Vereinbarungen über die konkrete Nutzung der Community Cloud zwischen den Beteiligten grundsätzlich leichter schließen, als das zwischen einem Private Cloud- und einem Public Cloud-Betreiber möglich ist.

Die kleinste Ausprägung einer Cloud – sofern sie diese Bezeichnung überhaupt verdient – ist die individuelle, die Personal Cloud. Hierbei steht weniger der Aspekt der Skalierung im Vordergrund als vielmehr die Möglichkeit, von vielen Rechnern aus auf gemeinsame Ressourcen – insbesondere Daten – zugreifen zu können. Mit einer zentralen Datenquelle stehen die Daten und Dienste jederzeit und auf allen Geräten mit Zugriff auf die zentralen Komponenten zur Verfügung. Dadurch werden langwierige Synchronisationsprozesse nur noch dann nötig, wenn ein Gerät längere Zeit ohne Verbindung zur Personal Cloud betrieben wird.

IaaS – PaaS –SaaS

Die o. g. Formel „Cloud = Grid + SaaS“ hat auf der rechten Seite zwei Parameter. Dies legt nahe, Cloud-Modelle weiter danach zu differenzieren, in welchem Umfang sie diese beiden entsprechenden Komponenten nutzen. Steht der Grid-Aspekt, also die vernetzte und skalierbare Hardware, im Vordergrund,

spricht man davon, dass Infrastruktur als Dienst bereit gestellt wird – auf Englisch „Infrastructure as a Service“, kurz „IaaS“.

Softwarenentwickler können solche Infrastrukturen z. B. nutzen, um ihre Produkte darauf zu entwickeln und zu testen, ohne evtl. komplexe Hardwaresysteme aufbauen zu müssen. Ein weiterführendes Cloud-Modell stellt dafür nicht nur die Infrastruktur bereit, sondern ganze Laufzeitumgebungen. Diese können z. B. Webserver, Datenbanken und Programmier-Frameworks umfassen, die zusammen eine Plattform für Entwicklung, Test oder andere Anwendungen bilden. Entsprechend wird ein solches Plattform-Angebot einer Cloud als „Platform as a Service“ – kurz „PaaS“ – bezeichnet.

Liegt der Schwerpunkt der Cloud-Dienste auf der „fachlichen“ Nutzung von Software – also z. B. Textverarbeitung, Kalenderfunktion oder Gehaltsabrechnung – wird das Cloud-Modell „Software as a Service“ – kurz „SaaS“ – genannt. Hier wird ggf. die Entkopplung von Funktionalität, die dann häufig über einen Web-Browser genutzt wird, und von Technik, die im Wesentlichen in der Cloud steckt, besonders deutlich. Auch die Daten verbleiben zumeist dort und können so von verschiedenen Endgeräten aus genutzt werden.

Unabhängig davon, auf welcher Ebene – Infrastruktur, Plattform oder Software – Cloud-Dienste angesiedelt sind, und unabhängig vom Betreibermodell – Public, Private, Community oder Hybrid – ist eine Eigenschaft charakteristisch für Cloud Computing: Durch sog. „Selbstzuweisung“ der Leistungen können Anwender sehr einfach die benötigten Dienste beziehen und auch wieder abbestellen. Innerhalb relativ kurzer Zeit werden Infrastrukturkomponenten, Plattformen oder Anwendungen eingerichtet bzw. aus dem Betrieb genommen. Das bedeutet auch, dass nicht jeder IT-Verbund, der gemeinsame Ressourcen zur Verfügung stellt, direkt auch eine Cloud darstellt.

Sicherheit

Geben und Nehmen

Wenn man Umfragen zum tatsächlichen oder geplanten Einsatz von Cloud Computing in Firmen liest, zieht sich ein Thema wie ein roter Faden durch die Ergebnisse: Auch wenn die Zahlen schwanken, sieht ein großer Teil der jeweils Befragten ein erhöhtes Sicherheitsrisiko in diesem Ansatz. Insbesondere, wenn es um den Schutz der eigenen Daten geht, herrscht große Skepsis. Das ist bei denjenigen Cloud-Modellen auch sofort nachvollziehbar, bei denen die Daten den eigenen Zuständigkeitsbereich verlassen. Zusätzliche technische Schnittstellen bei der Anbindung eines Providers stellen ein zusätzliches Bedrohungspotenzial dar. Organisatorische Schnittstellen für betriebliche und andere Prozesse sowie rechtliche Aspekte zum Datenschutz und zur Compliance werfen Fragen nach der Sicherheit auf, die beantwortet werden sollten, bevor Cloud-Dienste genutzt werden.

Dabei bietet Cloud Computing durchaus die Chance, die IT-Sicherheit für Daten und Anwendungen zu erhöhen. Für kleine und mittlere Organisationen, die sich keine ausgefeilte Sicherheitsorganisation und Sicherheitstechnik leisten können – oder gar für das Thema nicht sensibilisiert sind –, stellen die Basisvorkehrungen eines Cloud-Providers für die Sicherheit evtl. schon eine erhebliche Verbesserung dar. So kann z. B. ein Server, auf dem „unter dem Schreibtisch“ unternehmenskritische Anwendungen betrieben werden, durch die Verlagerung auf eine virtuelle Maschine in einem Rechenzentrum mit kontrolliertem Zugang besser gegen einen versehentlichen oder gezielten Eingriff am Gerät geschützt werden. Auch weiterführende Sicherheitsmaßnahmen dürften bei einem Cloud-Provider deutlich besser ausgeprägt sein als bei einem Unternehmen, in dem die IT nicht unmittelbarer Unternehmenszweck ist, sondern lediglich als Arbeitsmittel dient. Schließlich ist für Cloud-Provider das Vertrauen der Kunden in den sicheren Betrieb essenziell für ihr Geschäft.

Trotzdem sind die eingangs genannten Befürchtungen um die Sicherheit der eigenen Daten nicht aus der Luft gegriffen. Dafür gibt es mehrere Gründe: Die Sicherheit „von der Stange“ mag zwar gegenüber manch einem Betriebsszenario eine Verbesserung darstellen. Kunden mit spezifischen Sicherheitsanforderungen haben es aber schwer, diese in individuellen Servicevereinbarungen unterzubringen. Da Cloud Computing insbesondere davon lebt, dass die angebotenen Dienste schnell gebucht und eingerichtet, aber auch wieder abgesetzt werden können, sind Einzelvereinbarungen für jeden Anwendungsfall nicht praktikabel. Ein Weg dafür, Produkt- und Dienstleistungsspezifikationen einfach zu beschreiben und zu vereinbaren, ist es, sie in die Allgemeinen Geschäftsbedingungen zu schreiben. Für viele Verwaltungsanwendungen sind solche Standardklauseln aber nur bedingt geeignet, da häufig die Anforderungen des Datenschutzes und der Vertraulichkeit besondere Maßnahmen erfordern.

Ein weiterer Grund zur Skepsis gegenüber der Sicherheit von Cloud Computing hängt ebenfalls mit der Standard-Sicherheit zusammen. Der Nutzer der Cloud ist und bleibt für die Sicherheit seiner Daten und seiner Anwendungen verantwortlich. Sofern er lediglich Infrastrukturdienste nutzt, kann er zwar bis zu einem gewissen Grad davon ausgehen, dass diese angemessen geschützt sind. Und auch die Betriebsprozesse beim Provider folgen ggf. etablierten Prozessmodellen. Alle spezifischen Anwendungen und Dienste, die er auf dieser Infrastruktur nutzt, muss der Anwender aber selbst absichern. D. h., spezifisches Sicherheits-Know-how ist auf seiner Seite trotzdem erforderlich. Dies schränkt wiederum das Argument ein, mit der Verlagerung in die Cloud würde eine ausgefeilte Sicherheitsorganisation beim Anwender überflüssig. Der Bezug von externen Cloud-Dienstleistungen kann unter dem Gesichtspunkt der IT-Sicherheit erst dann vereinfacht werden, wenn es allgemeine Standards für deren Zertifizierung gibt, die verschiedene Schutzbedarfe berücksichtigen. Dann können ggf. angemessene Angebote miteinander verglichen werden.

Schließlich verschwinden reale und konkrete Bedrohungen für IT-Systeme und -Dienste nicht dadurch, dass man sie in der Cloud virtualisiert. Die klassischen Angriffsmethoden können auch dort zu Störungen führen. Dazu kommen neue Angriffstechniken auf der Ebene der virtuellen Systeme. Informationszentrierte Sicherheit kann hier zwar einen gewissen Schutz bieten (➔ HZD-Trendbericht 2010 „Informationszentrierte Sicherheit und Cloud Computing“), solange aber entsprechende Maßnahmen nicht angemessen implementiert sind, bieten auch Cloud-Systeme Angriffsflächen. So gelang es Forschern z. B., mit Hilfe von manipuliertem XML-Code virtuelle Maschinen in einer großen kommerziellen Public Cloud zu manipulieren. Durch sog. Cross-Site-Scripting gelang es ihnen zudem, einzelne Web-Service-Sessions in einer Web-Shop-Umgebung zu übernehmen.

Da sich die aufgezeigten Risiken nicht generell und nicht einfach beseitigen lassen, findet man häufig den Hinweis, komplexere und kritische Anwendungen in einer Private Cloud anzusiedeln und Dienste einer Public Cloud nur dann zu nutzen, wenn deren Nutzung vollkommen unkritisch ist.

Ausfälle und Störungen

Die Beschreibungen der verschiedenen strategischen Cloud-Modelle und der Service-Ebenen deuten schon an, dass Cloud-Umgebungen hochgradig komplexe Systeme darstellen können. Was für manch einen Nutzer entsprechender Anwendungen wie ein kleiner Dienst aussehen mag – ein wenig Speicherplatz, ein Kalender oder ein Adressverzeichnis, eine einfache Textverarbeitung – ist beim Cloud Computing nur ein kleiner Bruchteil umfangreicher Hardware-, Software- und Management-Systeme. Auf der einen Seite resultieren aus dieser Komplexität gerade die Vorteile des Cloud Computing: Wenn viele Nutzer sich viele Ressourcen teilen, kann jeder seinen Anteil relativ kostengünstig bekommen. Auf der anderen Seite bieten umfangreiche Systeme auch viele Möglichkeiten für Störungen: Selbst wenn nur einzelne Komponenten ausfallen, können schnell viele Nutzer betroffen sein und durch Seiteneffekte können sich derartige Störungen über die gesamte Cloud-Infrastruktur ausdehnen. So führte

vor kurzem bei einem großen Mailprovider der Ausfall einer Netzkomponente zu einem Rückstau von Nachrichten. Dieser dauerte – obwohl die defekte Komponente nach relativ kurzer Zeit wieder repariert war – mehrere Tage und blockierte den Maildienst für zahllose Nutzer.

Im vergangenen Sommer kam es bei zwei großen Cloud-Betreibern, die ihre Rechenzentren in der gleichen Region betreiben, durch einen großflächigen Stromausfall zu massiven Störungen ihrer Dienste. Während der eine Betreiber seine Office-Anwendungen nach wenigen Stunden wieder zur Verfügung stellen konnte, hielten die Auswirkungen bei den Infrastrukturdiensten des anderen bis zu zwei Tagen an. In diesem Fall waren u. a. Anwender betroffen, die ihrerseits Cloud-Anwendungen auf den gemieteten Infrastrukturen anbieten.

Es gibt noch eine Reihe von weiteren Berichten über Ausfälle verschiedenster „Dienste aus der Wolke“. Jede einzelne Störung mag noch vergleichsweise „normale“ Ursachen in einzelnen Komponenten gehabt haben. Durch die große Zahl abhängiger Komponenten und die Masse der Nutzerdaten in den Systemen waren deren Auswirkungen aber vielerorts gleichzeitig spürbar. Die Berichte zu den verschiedenen Störungen liefern einige Hinweise auf die Beschaffenheit von und auf den Umgang mit Cloud-Systemen:

- Fehler in einzelnen Komponenten können schwerwiegende Störungen „in der Fläche“ nach sich ziehen.
- In sehr großen komplexen Systemen ist die „Verkettung unglücklicher Umstände“ wahrscheinlicher als in kleinen Systemen.
- Der Ausfall von Notfallsystemen (z. B. Stromversorgung) ist möglich.
- Großflächige Störungen erfordern oft das manuelle Eingreifen der Systembetreuer, da Sicherungsmechanismen nicht oder anders als geplant funktionieren.

Während diese Punkte eher die Betreiber von Cloud-Technik betreffen, gibt es auch für die Anwenderseite wichtige Erkenntnisse. So zeigten die Störungen, dass die Verlagerung von Anwendungen in die Cloud nicht gänzlich davon entbindet, IT-Know-how vor Ort zu behalten. Die Berichte zu den o. g. Störungen enthalten mehrere Hinweise darauf, dass zur zeitnahen Umgehung der Probleme auf Seiten der Anwender Eingriffe in die Systemtechnik vorzunehmen waren. So sollten in einem Fall bestimmte Systemdateien gelöscht werden. In einem anderen Fall sollten Anwendungsinstanzen in anderen Cloud-Segmenten gestartet werden. In beiden Fällen sind Kenntnisse der Systeme oder gar der Cloud-Architektur beim Anwender notwendig.

Auch beim Lesen von Service-Level-Vereinbarungen (SLAs) muss der Anwender ggf. mehr Einblick in Technik und Architektur der Cloud haben, als es auf den ersten Blick notwendig erscheint: Z. B. ist es wichtig zu verstehen, auf welche technischen Komponenten und Segmente oder auf welche Anwendungs- bzw. Störungssituationen sich Verfügbarkeitsangaben beziehen. Für den Nutzer ist es bei einer Störung z. B. egal, ob die Ursache in der Anwendung oder im Netzsegment lag. Für die Frage der Kompensation bei Störungen mögen solche Details dann aber ausschlaggebend sein. Ungeachtet der Frage, wie die wirtschaftlichen Folgen von Störungen in der Cloud auf Anwenderseite behandelt werden, scheinen die Cloud-Betreiber sehr daran interessiert zu sein, durch kleine Vergünstigungen – etwa Erlass von (Teil-)Gebühren über einen gewissen Zeitraum oder kostenlose Softwarepakete – ihre Kunden zu beschwichtigen.

Bedrohungen aus der Wolke

In einem 1957 erschienenen Science Fiction-Roman – „The Black Cloud“ von Fred Hoyle – bedroht eine große schwarze Wolke das Leben auf der Erde. Auch wenn das Cloud Computing an sich zunächst keine Bedrohung für die Menschen oder die IT allgemein darstellt, können konkrete Bedrohungen aus der Wolke und deren Rechenleistung resultieren. Z. B. lassen sich virtualisierte Anwendungen massenhaft nutzen, um Passwörter durch sog. „brute force“-Angriffe – sprich: durch Ausprobieren von Wortvariationen – zu knacken. So wurde beispielsweise ausgerech-

net, dass zum Knacken eines üblichen WLAN-Passwortes kommerzielle Cloud-Rechenleistung für 1,68 US-Dollar reicht, und das Ergebnis nach ca. sechs Minuten vorliegen kann.

Werden solche Angriffe nicht rechtzeitig bemerkt, ist es später sehr schwierig, sie zu rekonstruieren, da alle Spuren schnell verwischt werden können. Dabei ist das gar nicht einmal auf besondere Bemühungen der Angreifer zurückzuführen. Werden die von ihnen zuvor genutzten Ressourcen anderen Anwendern zur Verfügung gestellt, können Daten des Angriffs aufgeteilt und schnell überschrieben werden.

Cloud Computing im öffentlichen Bereich

Sicherheit stellt also bei Cloud-Systemen einen kritischen Bereich dar. So verwundert es nicht, wenn im öffentlichen Bereich der Schwerpunkt von Cloud-Aktivitäten auf den sog. „Private Clouds“ liegt. Dabei werden die Leistungen des Cloud Computing einer geschlossenen Benutzergruppe im eigenen Verantwortungsbereich einer IT-Organisation angeboten (s. o.), und es ist wichtig, dass Cloud-Angebote über zwei Parameter skalieren können: über die Nutzerzahl und über die Zahl möglicher verwandter Dienste. Da in geschlossenen Benutzergruppen die Nutzerzahl begrenzt ist, müssen Private Clouds ihre Synergien aus der Technik bzw. der Anwendungsarchitektur gewinnen: Anstelle jeweils spezifischer Systeme und Anwendungen für einzelne Behörden oder gar Dienststellen werden Leistungen möglichst standardisiert und unter Nutzung gemeinsamer Ressourcen bereitgestellt. Im Bereich der öffentlichen Verwaltung bietet es sich dabei natürlich an, über Verwaltungsgrenzen und Zuständigkeiten hinaus weiterzudenken und Leistungen für viele Organisationen oder ggf. im Verbund mit mehreren Organisationen anzubieten. Im zweiten Fall betreiben diese Organisationen dann eine Community Cloud (s. o.).

Die Voraussetzungen für den sinnvollen Einsatz einer Private Cloud bzw. einer Community Cloud sind gerade im Bereich der öffentlichen Verwaltungen besonders gut erfüllt: Es gibt vielerorts gleiche bzw. eng verwandte Aufgaben. Die Verwaltungen vertrauen sich in der Regel gegenseitig, weil sie erstens sich nicht in einer Konkurrenzsituation zueinander befinden, zweitens vergleichbare Datenschutz- und oft auch Sicherheitsrahmenbedingungen haben und drittens im Rahmen übergreifender Verfahren oft schon mehr oder weniger eng zusammenarbeiten.

Die Themenfelder, die über den Erfolg von Clouds in der öffentlichen Verwaltung entscheiden, sind die gleichen, die auch im privatwirtschaftlichen Bereich bzw. bei Public Clouds eine wesentliche Rolle spielen:

Infrastruktur: Die gemeinsame Nutzung von Infrastrukturkomponenten kann in der Verwaltungs-IT ebenso beim Abfedern von Lastspitzen wie bei der Überbrückung von Ressourcenengpässen helfen, wie in der Privatwirtschaft.

Einrichtung: Der Aufbau von mehreren Private Clouds in der Verwaltung könnte werkzeugunterstützt und in abgestimmter Weise erfolgen. Dies würde Kooperationen bei der Verknüpfung von Angeboten und beim Aufbau einer Community Cloud erleichtern.

Management: In großen Clouds mit vielen Standardanwendungen aber auch dann, wenn Spezialanwendungen in einer Cloud passgenaue Ressourcen suchen, ist das Management der Cloud-Infrastrukturen wichtig. Dies gilt insbesondere dann, wenn bei der Zuordnung von Anwendungen und Ressourcen Zuständigkeitsgrenzen überschritten und die Aufgaben an Dritte delegiert werden. Dazu sind ggf. spezielle Technologien bzw. Produkte einzusetzen.

Netzwerkdienste: Will man Ressourcen verschiedener Anbieter schnell und flexibel nutzen, werden ebenso schnelle wie flexible Verbindungen zwischen verschiedenen technischen Systemen, Infrastrukturkomponenten, Diensten oder Anwendungen benötigt. Dies stellt die vorhandenen Netzwerke vor zusätzliche Herausforderungen.

Anwendungen: Die Zahl der Anwendungen, die identisch oder zumindest in vergleichbarer Form von

verschiedenen Verwaltungen genutzt werden, dürfte schwer zu ermitteln sein. Abgesehen von Standard-Büroanwendungen oder etwa kaufmännischer Software dürfte es bei den spezifischen Verwaltungsanwendungen eine Vielzahl von verschiedenen Softwaresystemen und Konfigurationen geben. Hier müssten beim Aufbau von Private oder Community Clouds diejenigen Anwendungen identifiziert werden, die am meisten von den Eigenschaften des Cloud Computing profitieren.

Sicherheit: Das Thema Sicherheit spielt beim Cloud Computing eine besondere Rolle (s. o.). Da einerseits öffentliche Verwaltungen sich gegenseitig vertrauen und es andererseits gemeinsame Bemühungen um die Sicherheit von IT-Infrastruktur gibt, bietet sich der Einsatz von Private oder Community Clouds an.

Fazit

Cloud Computing ist ein vielschichtiges Thema. Es hat sich in den vergangenen Jahren ständig weiterentwickelt. Euphorische Werbeartikel wie kritische Berichte und Risikobetrachtungen wechseln sich ab und tragen dazu bei, dass das Produkt – oder besser die Produktfamilie –„Cloud“ ein schärferes Profil bekommt. Und wie so oft liegt auch zum Einsatz von Cloud Computing die Empfehlung beim goldenen Mittelweg. Genauso wenig, wie man die uneingeschränkte Verlagerung von Diensten und Anwendungen in die Wolke empfehlen kann, kann man auch nicht generell davon abraten. Im einen Fall würde man Risiken verdrängen, im anderen Fall Chancen vergeben. Und schließlich ist die Palette der Lösungsmöglichkeiten zu groß, um eine allgemeingültige Empfehlung zu formulieren.

Die Antwort auf die Frage, ob man „in die Cloud gehen“ soll, hängt von vielen Faktoren ab:

- Welche Dienste und Anwendungen kommen dafür grundsätzlich in Frage?
- Wie sieht deren Schutzbedarf aus?
- Welches Betreibermodell ist unter fachlichen, technischen, rechtlichen und organisatorischen Gesichtspunkten geeignet und realisierbar?
- Welche Rahmenbedingungen für eine Wirtschaftlichkeitsanalyse gibt es?

Für einen strategischen Zugang zum Cloud Computing ist also eine umfassende Anforderungsanalyse der erste zentrale Schritt. Auch wenn diese Analyse es nahelegt, Cloud Computing in bestimmten Fällen zu nutzen, dürfte die Umsetzung allein durch Auswahl einer Lösung nicht so einfach möglich sein. Eine vergleichende Bewertung konkreter, in Frage kommender Lösungen wird mangels Qualitätsstandards auf diesem Gebiet zunächst schwierig sein. Und allein aufgrund der „Papierlage“ lassen sich Angebote nur bedingt bewerten und vergleichen. Solange sich Lösungskonzepte, Produkte und Standards rund um das Cloud Computing noch dynamisch entwickeln, kann es hilfreich sein, mit kleinen unkritischen Projekten zur internen Virtualisierung oder auch zur Nutzung externer Cloud-Dienste praktische Erfahrungen zu sammeln, um umfassendere Angebote Dritter besser einschätzen zu können.

Bewertung

Nach dem derzeitigen Stand scheinen Private und Community Clouds die für öffentliche Verwaltungen am besten geeigneten Modelle zur Virtualisierung von Infrastrukturen, Plattformen oder Anwendungen zu sein. Sie versprechen einen guten Kompromiss zwischen dynamischer Ressourcennutzung und dem Sicherheitsbedürfnis vieler Verwaltungen. Insbesondere für Verwaltungen gibt es dabei zwei Fragen, die über die o. g. allgemeinen Aspekte von Cloud Computing hinaus von Bedeutung sind: Wie werden zum einen in Modellen mit mehreren Partnern die vermeintlichen Überkapazitäten gesteuert, die ggf. Investitionen für die Nutzung durch Dritte erfordern? Und wie wird zum anderen die Selbstzuweisung von Ressourcen organisiert, so dass sie einerseits flexibel erfolgen kann, andererseits aber auch den Regeln für wirtschaftliches und sachgerechtes Verwaltungshandeln folgt.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Anwendungen & Web

Die Welt ist mein Büro – Web-Office

Über die Mobilisierung der Arbeit wurde schon viel geschrieben. Zunächst lag der Schwerpunkt der Bemühungen um die räumliche Loslösung der Arbeit vom Büro darauf, die Geräte für den täglichen EDV-Einsatz möglichst – im wahrsten Sinne des Wortes – tragbar zu gestalten. Von den großen Kisten, die mit ihren Tragegriffen eher einer Kühlbox für Getränke glichen und auch ein ähnliches Gewicht hatten, bis zu klappbaren Laptops war es zunächst ein relativ kleiner Sprung. Während jedoch die klobigen „Portables“ noch heute im Wesentlichen in Spezialanwendungen – z. B. mobilen Labors – zum Einsatz kommen, haben sich die Laptops im Lauf der Zeit ständig zu immer kleineren und leichteren Alltagsgeräten entwickelt. Bei ihnen liegt das Verhältnis von Rechenleistung zu Gewicht heute um den Faktor 500 höher als noch zu Beginn der Entwicklung vor etwa 25 Jahren. Nachdem man heute also angemessene Rechenleistung und die Darstellung auf einem vernünftigen Bildschirm auf kleinem Raum im Griff – und nicht mehr am Griff – hat, hat in den letzten Jahren die mobile Vernetzung an Bedeutung gewonnen (➔ u. a. „LTE – Long Term Evolution“).

Sowohl im beruflichen als auch im privaten Umfeld sind Computer heute in der Regel in Netze eingebunden und können Informationen aus aller Welt abrufen. In vielen Regionen der Industriestaaten gehört der mobile Zugang zum Internet und über gesicherte VPNs in Firmennetze zum Alltag. Dennoch sehen Anwender – und auch Anbieter von Netzdiensten und Software – noch weiteren Optimierungsbedarf für das Arbeiten „jederzeit und überall“: Wer nicht gerade Bürorechner und Privatrechner in einem Gerät vereint hat, steht schnell vor der Frage, ob er auf eine Reise nicht vielleicht doch beide Geräte mitnehmen soll. Aber die Arbeit im Strandcafé wirkt auch wieder nur halb so entspannt, wenn man dort mehrere Computer aufbaut. Also muss man sich entscheiden, ob man die Büroumgebung oder doch lieber die moderneren Anwendungen der neuesten Generation vom Privatrechner nutzen möchte, die am Arbeitsplatz noch nicht „ausgerollt“ sind. Spätestens jetzt kann der Wunsch entstehen, nicht nur die Technik und die Daten zu mobilisieren, sondern auch die Anwendungen.

Dank der heute leistungsfähigen Netzwerke und weit entwickelter Netzprotokolle und -sprachen können inzwischen auch „Büroanwendungen“ wie Textverarbeitung, Tabellenkalkulation oder Präsentationsprogramme online zur Verfügung gestellt und genutzt werden. Das scheint sowohl für Anwender wie auch Lieferanten Vorteile zu haben: Der Nutzer kann überall, wo eine Internetverbindung vorhanden ist, und mit jedem Gerät, das über einen Standardbrowser verfügt, auf „seine“ Anwendungen zugreifen. Und wenn die Daten dann auch noch „in der Cloud“ liegen, steht dem universellen Arbeitsplatz praktisch nichts im Wege. Selbst Spezifika eines Betriebssystems fallen ggf. weniger ins Gewicht als bei lokalen Anwendungen. Und um die Aktualisierung von Funktionen und Sicherheitsmechanismen muss sich der Anwender auch nicht mehr selber kümmern, sondern nutzt jeweils die aktuellste Version der Programme. Für die Anbieter von derartiger Standardsoftware könnte sich dieser Ansatz ebenfalls lohnen: Zum einen vereinfachen sich die Vertriebswege, da weder Datenträger noch gigabyteschwere Downloads bereit gestellt werden müssen. Zum anderen hat der Anbieter des Dienstes die Kontrolle über die Nutzung der Software und kann damit über ein entsprechendes Kostenmodell seine Erlöse steuern. Das klassische Raubkopieren von Software ist nicht mehr möglich.

Derzeit sieht die Praxis aber noch ein wenig anders aus: Die reinen Web-Alternativen zu lokalen Büroanwendungen verfügen in der Regel über einen sehr eingeschränkten Leistungsumfang. Dadurch ist es für die Anbieter zwar möglich, relativ einfach zu bedienende Anwendungen kostengünstig – oder gar kostenlos – bereitzustellen, jedoch wird der geübte Anwender schnell gewohnte Funktionen vermissen. Insofern bleibt zunächst die Zweiteilung der Arbeitswelt bestehen: hier professionelles Arbeitswerkzeug mit spezifischer Anwendungssoftware, dort eine einfache Web-Alternative – um nicht zu sagen „Notlösung“. Aus dieser Teilung ergeben sich evtl. wiederum Fragen der Datenkompatibilität. Selbst wenn Dokumente auf offenen Standards basieren, besteht

zumindest bei deren Übertragung in eine einfacher strukturierte Umgebung die Gefahr, dass komplexe Dokumenteigenschaften auf der Strecke bleiben. So verfügen z. B. sehr einfache Textanwendungen zwar ggf. über Formatvorlagen, aber evtl. nur für wenige Textarten wie Fließtext und Überschriften, die sich auch nicht vom Nutzer um weitere Vorlagen ergänzen lassen.

Wer mit etwas eingeschränktem Funktionsumfang gut leben kann, kann mit den Web-Werkzeugen für die Büroanwendungen ggf. von einer weiteren Möglichkeit profitieren, die die Arbeit im Netz bietet: Manche Office-Anwendungen unterstützen die parallele Arbeit durch verschiedene Nutzer an einem Dokument. So ist es möglich, auch über größere Entfernungen an gemeinsamen Formulierungen zu arbeiten, ohne das Dokument ständig per E-Mail hin- und herschicken zu müssen. Bei einem solchen Einsatz sind dann ggf. auch die eingeschränkten Funktionen der Textverarbeitung zu verschmerzen. Die abschließende Gestaltung des inhaltlich abgestimmten Ergebnisses kann später mit dem komplett ausgestatteten Programm lokal erfolgen.

Bewertung

Die Antwort auf die Frage nach dem Einsatz webbasierter Office-Anwendungen in öffentlichen Verwaltungen wird bisher eher noch von anderen Faktoren bestimmt, als dass sie eine reine Produktentscheidung wäre. Solange die Webanwendungen keine vollständigen Office-Produkte sind und zu den ggf. noch benötigten lokalen Anwendungen nur eingeschränkt kompatibel sind, können sie nicht als strategische Standardprodukte eingesetzt werden. Ungeachtet dessen müssen aber auch die Rahmenbedingungen und Einsatzszenarien bedacht werden, in denen Webanwendungen genutzt werden könnten. Da stellen sich einerseits Fragen zur Sicherheit und zum Datenschutz: Wo liegen die Daten und auf welchen Wegen erfolgt der Zugriff darauf? Andererseits müssen evtl. reduzierte Betriebsaufwände gegen erhöhte Schulungs- oder zumindest Einarbeitungsaufwände abgewogen werden, wenn die Entscheidung über die eingesetzte Programmversion in fremde Hände gelegt wird. Und schließlich ist abzuwägen, in welchen Anwendungsfällen und in welchem Umfang die Verwaltung – oder Teile davon – von der Mobilisierung der Anwendungen profitieren kann. In einer hinreichend abgesicherten Betriebsumgebung und in definierten Szenarien können Weboffice-Anwendungen aber zumindest eine hilfreiche Ergänzung zur sonst üblichen Arbeitsumgebung sein.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit*:	
Marktreife/Produktverfügbarkeit:	

** für den reinen Produkteinsatz*

Social Media als Mail-Ersatz?

Seit Computer miteinander vernetzt werden, besteht der Wunsch der Nutzer, über dieses Medium Nachrichten miteinander auszutauschen. Daher lohnt sich auch im Hinblick auf die aktuellen Entwicklungen der elektronischen Kommunikation ein Blick in deren Geschichte. Im amerikanischen ARPANET, dem Urvater des Internets, wurde bereits 1971 dafür das Mail-Box-Protocol entwickelt, 1973 folgte FTP Mail auf der Basis des File Transfer Protocols. Die E-Mail, wie wir sie heute kennen, begann Anfang der 1980er Jahre mit der Trennung des Nachrichtendienstes von der Datenübertragung per FTP, und das auch heute noch zugrunde liegende Simple Mail Transfer Protocol, SMTP, wurde bereits zu dieser Zeit entwickelt. Seither wurden eine Vielzahl von Mailservern und eine noch größere Zahl von Mailclients zum Lesen und Schreiben von Nachrichten entwickelt, die zwar zunehmend über immer mehr Funktionen wie strukturierte Ablageordner, automatische Archivierung oder „intelligente“ Adressbücher verfügen, die aber doch im Kern der Verarbeitung von einfacher E-Mail dienen.

Aber auch die Entwicklung anderer computergestützter Kommunikationsformen reicht bis in diese Zeit zurück. Der Austausch von Informationen in Gruppen wurde auf Großrechnern mit dem Betriebssystem MULTICS bereits 1969 realisiert. Im sog. „Continuum“ konnten an Pinnwänden (engl. Bulletin Boards) themenorientiert Nachrichten verbreitet werden, auf die berechtigte Nutzer Zugriff hatten.

In der UNIX-Welt entwickelte sich ab 1979 ein ähnliches System von themenzentrierten Diskussionsgruppen, die über das sog. USENET miteinander vernetzt wurden. Die einzelnen Beiträge – die News – werden von den Newsservern verbreitet und können mit Hilfe von Newsreadern gelesen werden. Im USENET entstanden auch die „Benimmregeln“ für elektronische Kommunikation – die sog. Netiquette.

Als modernes Abbild von Pinnwänden und Newsgroups im Internet können Webforen gesehen werden, wenngleich es hinsichtlich der technischen Verbreitung der Nachrichten Unterschiede gibt. Während man die USENET-Gruppen in der Regel von einem einzigen Server abonniert, werden verschiedene Webforen normalerweise auf unterschiedlichen Servern bereitgestellt. Auch in der Darstellung der Angebote gibt es wesentliche Unterschiede: Der Newsreader – das Programm zum Lesen und Schreiben von USENET-Nachrichten – übernimmt die Darstellung und vereinheitlicht sie über alle Gruppen hinweg. Das Aussehen von Internetforen – wie auch deren Funktionsumfang – unterliegt dagegen der Kontrolle des jeweiligen Anbieters und soll vom Webbrowser möglichst „authentisch“ abgebildet werden. Damit ergibt sich eine ähnlich breite Palette an „Webanwendungen“ für Foren wie bei E-Mail-Programmen.

Viele heutige Soziale Netze bzw. Soziale Medien kombinieren die öffentliche bzw. „gruppenöffentliche“ Kommunikation mit der Möglichkeit, persönliche Nachrichten auszutauschen. Sie können also aus der Kommunikationsperspektive grob als ein Gemisch aus Mail- und Forendiensten betrachtet werden – ggf. ergänzt um weitere Funktionen.

Zurzeit ist – zumindest in Deutschland – E-Mail noch das bevorzugte elektronische Kommunikationsmedium. Nahezu alle Internetnutzer haben auch eine E-Mail-Adresse, während nur rund 60 % von ihnen auch in sozialen Netzen aktiv sind. Eine aktuelle Prognose eines großen Marktforschungsunternehmens über die elektronische Kommunikation sagt jedoch voraus, dass in absehbarer Zeit die Nutzung von Sozialen Medien die Nutzung von E-Mail ablösen wird: Bereits in wenigen Jahren soll ein Fünftel der Firmenanwender die Dienste von Sozialen Netzen als primären Kommunikationskanal verwenden.

Eine so drastische Vorhersage ruft natürlich schnell die Kritiker auf den Plan, die dann anführen, dass Soziale Medien die E-Mail schon deshalb nicht verdrängen werden, da solche Medien in der Regel eine funktionsfähige Mailadresse bei der Registrierung voraussetzen und E-Mail auch oft zur Benachrichtigung über Änderungen der Sozialen Medien verwendet werden. Solche Begründungen sind nur bedingt tragfähig – wie auch das Argument, dass viele Menschen den modernen Medien und Netzwerken sehr kritisch gegenüberstehen. Ein weiteres Argument lenkt den Blick allerdings auf ein Thema, das im Zusammenhang mit der Kommunikation über Soziale Netze eine wesentliche Rolle spielt. Es handelt sich dabei um die Beobachtung der Kritiker, dass die Nutzung Sozialer Netze heute noch in vielen Unternehmen unterbunden wird, während die Kommunikation per E-Mail in der Regel möglich sei. Hier wird indirekt die Frage angesprochen, welche Sozialen Netze denn welchen Teil der E-Mail-Kommunikation – insbesondere von Unternehmen – ablösen werden. Steigt man tiefer in die Diskussion ein, sieht man, dass die Verschiebung der Kommunikationswege zunächst nur innerhalb einzelner Unternehmen prognostiziert wird. Hier kann der Übergang von der direkt adressierten Nachricht – wenn auch ggf. an größere Verteiler – zur firmenintern allgemein zugänglichen Nachricht, z. B. in einem Blog oder einem Forum, zu einem verbesserten Austausch von Wissen führen. Die bei einem Mikroblogging-Dienst sog. „Follower-Power“ – also die Schnelligkeit bei der Beantwortung von Fragen oder ähnlicher Unterstützung – löst evtl. Ketten von Abwesen-

heitsmeldungen und Weiterleitungen in etablierten E-Mail-Strukturen ab, wenn eine Anfrage an viele Mailadressaten geschickt wird. Aus Gründen des Datenschutzes und zur Sicherung von firmeninternen Informationen bietet es sich an, derartige Dienste im eigenen Netz anzubieten. Doch damit stellt sich sehr schnell die Frage nach der Kommunikation mit Kunden oder Lieferanten. Sofern die firmeneigene Lösung keine geeigneten Berechtigungsmechanismen zur Steuerung von Informationen besitzt, bietet sich spätestens bei diesen Partnern wieder die E-Mail als klassischer Kommunikationsweg an. Oder beide nutzen firmenexterne Soziale Netze zur Kommunikation. Dies wiederum wirft aber die Frage auf, wem die dort hinterlegten Kontaktinformationen und die ausgetauschten Nachrichten gehören. Während Kontaktinformationen schnell zu einem juristischen Zankapfel werden können, wenn ein Mitarbeiter eine Firma verlässt, stellt sich bezüglich der Nachrichten noch zusätzlich die Frage, ob und wie der Betreiber des Sozialen Mediums die Informationen nutzen darf. Dieses Thema scheint derzeit insofern brisant zu werden, als der Anbieter eines sozialen Netzes Informationen aus Nachrichten verwenden möchte, um darauf basierend gezielt Werbung verteilen zu können.

Abgesehen von solch grundsätzlichen Überlegungen stellen sich weitere Fragen bei der Veränderung von Kommunikationsstrategien in Unternehmen. Selbst wenn eigene Lösungen aufgebaut werden, werden die größten Herausforderungen nicht in der Technik, sondern in der Nutzung der neuen Dienste gesehen. Trotz des Wunsches, die halböffentliche Kommunikation hinsichtlich Qualität und Quantität nicht ausufern zu lassen, versuchen Unternehmen die Schwelle für die Nutzung der Dienste niedrig zu halten und die Kontrollen möglichst zu beschränken – etwa darauf, dass keine Kommunikation anonym erfolgen darf. Trotzdem werden den Projekten für die Einführung von sozialen Medien in Unternehmen nur geringe Erfolgsaussichten zugeschrieben: etwa 50 bis 70 % der Bemühungen sind laut Vorhersagen zum Scheitern verurteilt, weil die potenziellen Nutzer der neuen Dienste nicht angemessen eingebunden werden.

Während separate Netzwerke für geschlossene Nutzergruppen mit den Schwierigkeiten des Aufbaus zu kämpfen haben, streiten die allgemein zugänglichen Sozialen Netzwerke um die Nutzer und sind auf der Suche nach Geschäftsmodellen, mit denen sich diese Dienste langfristig finanzieren lassen. Insofern werden die verschiedenen Prognosen über die Ablösung der E-Mail durch Soziale Medien noch eine Weile warten müssen, bevor sie zutreffen – zumindest sofern es um die globale Kommunikation geht und nicht nur um den Austausch von Informationen in vergleichsweise kleinen Gruppen.

Die Frage, ob sich grundsätzlich neuartige Kommunikationskanäle etablieren werden, lässt sich vielleicht dann beantworten, wenn man sich die eingangs erwähnte Entwicklung der E-Mail-Programme noch einmal ins Gedächtnis ruft: Hier gibt es eine Vielzahl von unterschiedlichen Anwendungen, die in geschlossenen und auch offenen Netzen eingesetzt werden können und die mal mehr, mal weniger Zusatzfunktionen bieten. Kern und Grundlage bildet jedoch überall der zumindest standardisierte Mail-Dienst. Wenn es gelingt, Soziale Medien und die Kommunikation in Sozialen Netzen auf ähnlich standardisierte Strukturen aufzubauen, könnte dies tatsächlich zu neuen universellen elektronischen Kommunikationsdiensten führen. Bisher versuchen die Anbieter von Spezialanwendungen noch individuell, die verschiedenen Dienste unter einen Hut zu bekommen und Informationen aus Netzwerken und Mikroblogging in einer gemeinsamen Oberfläche zu integrieren. Dies gelingt den verschiedenen Anbietern unterschiedlich gut, und so ist zwischen den verschiedenen Plattformen ein deutlicher Wettstreit zu spüren, der sich im Zukauf von ergänzenden Diensten und in der (Nicht-)Durchlässigkeit von Informationen aus einem Konkurrenzprodukt niederschlägt. Die Nutzer stehen als mehr oder weniger loyale Fangemeinde einzelner Produkte dabei und orientieren sich nicht selten an dem, was gerade populär ist. In der Folge gibt es regelmäßig umfangreiche Abwanderungsbewegungen von einer Social Media-Plattform zur nächsten, vor denen auch die Branchengrößen nicht gefeit sind. So findet man immer wieder Meldungen, dass ein Bekannter kaum noch oder gar nicht mehr bei einem bestimmten Dienst zu finden

ist. Während die meisten E-Mail-Programme die Möglichkeit bieten, neue Mail-Adressen in einem zentralen Adressbuch zu pflegen, müssen sich die Nutzer von Social Media-Plattformen anderweitig merken, welcher ihrer Kontakte über welchen Dienst erreichbar ist. Solange die sozialen Medien nicht auf Basis von Standards für Nachrichten und Kontakte durchlässig werden, ist das Ende der E-Mail noch nicht abzusehen.

Bewertung

Nicht nur für Unternehmen, sondern auch für Verwaltungen stellt sich heute oft die Frage, ob E-Mail das in jedem Fall geeignete Kommunikationsmittel ist, oder ob es für spezifische Anwendungsfälle andere, besser geeignete Wege gibt. Soziale Medien gewinnen dabei zunehmend an Bedeutung – sowohl in der internen Kommunikation als auch in der Beziehung zu Verwaltungskunden. Vor dem Einsatz entsprechender Dienste ist aber genau zu prüfen, ob – und ggf. welchen – vorhandenen Kommunikationskanal man verwendet, oder ob man selber einen spezifischen Kanal aufbaut. Gerade bei der Kommunikation nach außen stellt sich dabei die Frage der Reichweite Sozialer Medien – also wie viele potenzielle Kunden man mit einem solchen Kanal erreichen kann. Während ein Blog mit der Möglichkeit Kommentare abzugeben evtl. noch genug Leser findet, bieten sich für die Kommunikation in Netzwerken eher bestehende Plattformen an. Dies setzt aber zum einen voraus, dass eine entsprechende Kommunikationsstrategie vorhanden ist – „Wer redet wo mit wem worüber?“. Zum anderen muss die Auswahl der Medien „diskriminierungsfrei“ sein, d. h. Kunden dürfen nicht zur Nutzung bestimmter Medien gezwungen werden, ohne die ihnen die Informationen nicht zur Verfügung stehen. Die verwaltungsinterne Nutzung sozialer Medien kann zumindest schon dazu beitragen, praktische Erfahrungen zu sammeln. Solange aber die Kommunikation mittels sozialer Medien noch nicht durch Standards über Plattformgrenzen hinweg harmonisiert ist, wird E-Mail für öffentliche Verwaltungen noch ein wesentlicher Kanal für die Kommunikation über reine Informationsverbreitung hinaus bleiben.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Anwendungen? Da gibt's doch was vom App-Store!

Apps sind derzeit in aller Munde – oder genauer gesagt: auf vielen Smartphones und anderen mobilen Geräten. Dabei steht „App“ als Abkürzung lediglich für „Applikation“ – also „Anwendung“. Letzten Endes sind Apps also nichts anderes als mehr oder weniger kompakte und leicht zu beziehende Anwendungen – insbesondere für mobile Geräte. Auf den zweiten Blick verbinden sich mit dieser Art von Anwendungen einige Trends, die zu beobachten angeraten ist. Das eine ist die starke Bindung an Betriebssysteme. Da Apps für mobile Geräte in der Regel mit recht begrenzten Ressourcen wie Rechenleistung, Speicher oder Bildschirmgröße zurechtkommen müssen, ist es naheliegend, sie so zu entwickeln, dass sie die vorhandenen Möglichkeiten möglichst gut ausnutzen. Dadurch sind viele Applikationen auf bestimmte Systemplattformen beschränkt oder werden nacheinander auf mehrere Betriebsumgebungen portiert. Das erscheint zwar unter dem Aspekt des Realisierungsaufwandes logisch, bedeutet aber gegenüber Anwendungen, die über – nahezu – beliebige Webbrowser nutzbar sind, wieder eine stärkere Bindung zwischen Soft- und Hardware. Dies mag bei Handys noch akzeptabel sein, solange es nur darum geht, einen Dienst „auch mal mobil“ nutzen zu können. Wenn es aber darum geht, komplexere Anwendungen im geschäftlichen Umfeld auf den neuen Tablets zu nutzen, kann das weiter reichende Konsequenzen haben: Entweder trifft man die strategische Entscheidung für eine bestimmte Systemplattform oder verwendet alternative Anwendungen, die auf bereits vorhandenen strategischen Plattformen

funktionieren. Oder aber man erweitert die Grenzen seiner Hard- und Softwarearchitektur so, dass alles dort möglich ist, wo es gebraucht wird. Im Hinblick auf die Administrier- und Beherrschbarkeit der Informations- und Kommunikationstechnik im Unternehmen – spätestens aber unter dem Gesichtspunkt der Sicherheit – stellt dieser letzte Ansatz erhöhte Anforderungen an Nutzer und Betreiber.

Mit der Kopplung von Soft- und Hardware hängt ein weiterer Trend zusammen: Apps werden zunehmend in speziellen virtuellen Geschäften, sog. App-Stores, angeboten. Der ursprüngliche Gedanke eines Herstellers von Handys und Tablets dabei war, dass man durch die Kontrolle der angebotenen Software größeren Einfluss auf die Funktionsfähigkeit der mobilen Geräte – insbesondere auch bei den Basisfunktionen – hätte. Für den Nutzer ergeben sich daraus sowohl Vor- als auch Nachteile: Auf der einen Seite ist es komfortabel, eine oder wenige zentrale Anlaufstellen zu haben, an denen man fast alle spezifischen Apps bekommen kann. Die Suche nach Anwendungen wird dadurch vereinfacht. Auf der anderen Seite tritt so bei der Beschaffung von Apps ein Zwischenhändler ins Spiel, der Einfluss auf Umfang und Kosten der Angebote hat.

Wie sich diese Trends rund um Apps weiterentwickeln, hängt stark mit der Entwicklung des Marktes für mobile Geräte zusammen: Neben der Platzierung von einzelnen Produkten, die für sich schon einen Trend darstellen und den Erwerb spezifischer Apps fördern, wird es umgekehrt das Angebot von Anwendungen sein, das das Kaufverhalten bei der Hardware beeinflusst. Ob dies zu einer Diversifizierung oder zu einer weiteren Spezialisierung auf dem Markt führt, ist derzeit noch offen. Das stellt Anbieter von Software und Datendiensten – insbesondere auch öffentliche Verwaltungen – vor Herausforderungen. Sie müssen sich mit den Fragen beschäftigen, ob sie ihre Leistungen auch in kleinen, bunt verpackten Softwarepäckchen bereitstellen wollen und ggf. auf welchen Plattformen. Während private Unternehmen bei der Wahl der Zielplattformen offen sind und diese von den – erwarteten – Bedürfnissen ihrer Kunden abhängig machen können, müssen öffentliche Einrichtungen darauf achten, dass sie durch die Wahl technischer Plattformen bzw. ganzer Zugangskanäle nicht diskriminieren, d. h. potenzielle Kunden ausschließen, die nicht über die entsprechenden Mittel verfügen. Sie müssen ggf. angemessene Alternativen – und seien sie papiergebunden – für diejenigen schaffen, denen die neuen Zugangskanäle nicht oder nur eingeschränkt zur Verfügung stehen.

Je weiter sich Apps verbreiten, desto mehr nehmen auch Diskussionen um die Zukunft dieser Technik bzw. Software-Architekturvariante zu. Dabei sind es z. T. die oben angesprochenen Rahmenbedingungen wie Hardware/Software-Kopplung, Geschäftsmodelle oder Sicherheit der App-Software, die die Frage aufwerfen, ob spezifische Apps oder doch wieder Webanwendungen – zu sog. Web-Apps benutzerfreundlich aufbereitet – in Zukunft den Markt für Anwendungssoftware bestimmen – zumindest im mobilen Bereich. Das Thema Apps wirft aber auch Licht auf weitere Fragen des mobilen Arbeitens, die nur mittelbar mit der Frage der Apps zu tun haben: Diese betreffen die Wahl technischer Plattformen (➔ „Bring your own Device“), mobile Anwendungen (➔ „Die Welt ist mein Büro – Web-Office“), Virtualisierung sowie grundlegende Fragen der Sicherheit. Die Zukunft von Apps liegt aber vermutlich wie immer in der Mitte: Apps, Webanwendungen und komplexe Standardanwendungen werden wohl noch einige Zeit parallel existieren und in spezifischen Anwendungsbereichen ihre Stärken ausspielen. Ob sich tatsächlich einmal ein einheitliches Modell für den Bau von Anwendungssoftware durchsetzt – mit oder ohne Apps –, hängt von weiteren Faktoren ab: Die Entwicklung von Hardware, Betriebssystemen und Netzwerken werden darauf einen wesentlichen Einfluss haben.

Bewertung

Für öffentliche Verwaltungen sind die Trends rund um Apps in zweierlei Hinsicht interessant: einmal aus der Sicht des potenziellen Nutzers und einmal aus der Sicht des Anbieters. Für die Nutzung stellt sich zum einen die Frage, welche Dienste sinnvollerweise als App bezogen werden können. Dies dürften i. d. R. allgemeine Dienste sein, die der Unterstützung der Arbeit dienen – Kommunikationswerkzeuge, Hilfen bei der Planung und Durchführung von Dienstreisen, Nachschlagewerke und andere Informationsangebote. Doch schon für solch vergleichsweise einfachen Apps sind zwei wichtige Dinge zu beachten: Das ist zum einen die Frage der Beschaffung, da auch niedrigpreisige Güter dem Vergaberecht unterliegen. Darüber hinaus können aber auch komplexere Anwendungen – z. B. sog. Office-Anwendungen – je nach benötigtem Leistungsumfang zum Einsatz kommen. Das andere ist die Frage nach der Sicherheit: Apps lassen sich i. d. R. sehr einfach und unmittelbar aus einem App-Store auf einem Endgerät installieren. Dies erschwert die Kontrolle der eingesetzten Softwarekomponenten in größeren Organisationseinheiten.

Für die Verwaltung als potenzieller Anbieter einer App stellt sich die Frage nach der jeweiligen Zielgruppe – insbesondere nach deren Größe – sowohl bei verwaltungsinternen Angeboten als auch Angeboten für Verwaltungskunden. Während man bei geschlossenen Gruppen i. d. R. Kontrolle über die technische Zielplattform hat, spielt der o. g. Aspekt der (technischen) Diskriminierung bei öffentlichen Angeboten eine größere Rolle. Hier muss ggf. geprüft werden, ob eine App auf mehreren Plattformen bereitgestellt werden soll.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Mobiles Bezahlen mit dem Handy

Die Erwartungen sind vielfältig: Ob mobiles Bezahlen mit dem Handy sich einmal im Alltag etablieren wird oder wieder in der Versenkung verschwinden wird, hängt davon ab, wen man dazu befragt. Zurzeit gibt es aber auf jeden Fall einige Entwicklungen, die nahelegen, dass das Thema zunächst an Bedeutung gewinnt.

Für das Bezahlen mit dem Handy gibt es verschiedene Methoden. Die einfachste davon besteht im Versenden einer SMS durch den Kunden, deren erhöhte Gebühren dann dem Anbieter gutgeschrieben werden. Dieses Verfahren ist besonders unkompliziert, da es auf Seiten des Käufers keine besonderen Anforderungen an Hard- oder Software stellt. Die Kosten werden über die Handyrechnung beglichen. Lediglich der Anbieter muss einen entsprechenden Dienst eingerichtet haben. Allerdings eignet sich diese Methode nur für einige feste Preise. Zudem verlangen entsprechende Dienstanbieter bis zu 50 % der SMS-Kosten als Gebühren.

Eine andere ebenfalls einfach zu handhabende Bezahlmethode sind Anrufe. Dafür muss der potenzielle Nutzer des Dienstes sich – bzw. seine Handynummer – beim Anbieter registrieren lassen. Mit einem einfachen Anruf lassen sich dann Stückkosten begleichen. Aber auch Leistungen nach Aufwand bzw. Verbrauch zu bezahlen, ist möglich. So können z. B. Parkgebühren bezahlt werden, indem zu Beginn und zu Ende des Parkens die entsprechende Nummer angerufen wird. Auch Leihfahrräder können auf diesem Weg gebucht werden: Beim ersten Anruf wird dem Kunden ein Code für das Fahrradschloss mitgeteilt. Am Ende der Fahrt ruft er wieder an und teilt den Ort mit, an dem das Fahrrad abgestellt wurde.

Die Übermittlung von Zugangscodes – als Zahlenkombination oder als grafische Codes wie z. B. QR-Codes – kann auch genutzt werden, um Eintritts-, Fahr- oder Flugkarten zuzusenden. Je nach Anwendung müssen dann Zahlencodes entweder an einem Terminal eingegeben oder – wie bei Online-Briefmarken – abgeschrieben werden. Grafische Codes werden mit Scannern vom Handy-Bildschirm abgelesen und überprüft.

Schließlich gibt es noch Bezahlmethoden, die mittels sog. Near Field Communication, NFC (vgl. HZD-Trendbericht 2008/2009), realisiert werden. Diese Funktechnik dient dazu, Daten über sehr kurze Entfernungen zu übertragen. Was zunächst wie ein Mangel an Reichweite erscheinen mag, ist beim Bezahlen aber Teil des Konzepts: Indem der Kunde sein Handy, das mit NFC-Technik ausgestattet sein muss, in die Nähe eines entsprechenden Lesers hält, werden die für den Zahlungsvorgang notwendigen Informationen übertragen. Die kurze Reichweite sorgt hier dafür, dass nicht „aus Versehen" Geschäftsvorfälle ausgelöst werden. Diese Technik wird in einem großflächigen Pilotversuch von Bahn und weiteren Verkehrsbetrieben erprobt: Registrierte Testpersonen bekommen ein NFC-fähiges Handy zur Verfügung gestellt, da es bisher in Deutschland kaum solche Geräte zu kaufen gibt. Wenn sie in den beteiligten Pilotregionen reisen, müssen sie sich zu Beginn ihrer Fahrt registrieren, indem sie das Handy an ein „Touchpoint" genanntes Terminal halten. Das Mobiltelefon liest von diesem die Standortdaten aus. Auch am Ziel der Reise werden die dortigen Informationen erfasst. Eine Anwendung berechnet dann anhand von Orten, Reisezeit und Kontrolldaten die zurückgelegte Strecke sowie genutzte Verkehrsmittel und damit den Preis.

Derlei Anwendungen für das mobile Bezahlen können sich gut 40 % der Handybesitzer vorstellen. Rund ein Viertel der Nutzer würde evtl. Eintrittskarten so bezahlen, jeder fünfte würde das Handy grundsätzlich zum bargeldlosen Bezahlen einsetzen. Doch die Realität sieht derzeit noch ganz anders aus: In Deutschland nutzen derzeit nur 1 % der Handybesitzer ihr Gerät tatsächlich zum Bezahlen. Mit 2 % ist der Anteil in den USA zwar doppelt so hoch, aber auch noch weit davon entfernt, dass man von einem Massenphänomen sprechen könnte. Nach anderen Umfragen wird sich dies auch nicht so bald wesentlich ändern, denn dabei gaben mehr als 70 % der Befragten in Europa und mehr als 60 % in den USA an, dass sie kein Interesse an dem Thema haben. Mehr Bewegung gibt es in Asien: In Japan bezahlen bereits 12 % der Handybesitzer mobil. Die größten Fortschritte macht das mobile Bezahlen per Handy aber in Entwicklungsländern. Dort gibt es häufig keine Infrastruktur für das Bezahlen mit Kredit- oder Scheckkarte. Dank der vorhandenen Funknetze kann hier aber dennoch auf relativ einfache Weise der bargeldlose Zahlungsverkehr ermöglicht werden.

Bewertung

Mobiles Bezahlen mit dem Handy wäre für öffentliche Verwaltungen grundsätzlich eine interessante Möglichkeit, ihre kostenpflichtigen Leistungen erstatten zu lassen, da diese bargeldlose Methode nahezu überall – insbesondere unabhängig vom Ort der Leistungserbringung – angeboten und flexibel eingesetzt werden kann. Bevor solche Lösungen aber umgesetzt werden, sollten mehr Erfahrungen – insbesondere in puncto Sicherheit – vorliegen.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Technik

Auf dem silbernen Tablet

Die Erwartungen der Technikbegeisterten sind bei jeder Neuankündigung hoch: Seit die Firma Apple mit ihrem iPad das Thema „Tablet-Computer“ erfolgreich neu belebt hat, haben alle einschlägigen Unternehmen große Anstrengungen unternommen, bei diesem IT-Trend dabei zu sein.

Die entsprechenden Messen der Informations- und Unterhaltungselektronik werden von diesem Thema rund um den „Notizblock-Computer“ („tablet“ engl. „Schreibtafel“, am.-engl „Notizblock“) in weiten Teilen beherrscht. Sowohl im Hardwarebereich – mit Konkurrenzprodukten – als auch im Softwarebereich – mit maßgeschneiderten Anwendungen (sog. „Apps“, ➔ „Anwendungen? Da gibt’s doch was vom AppStore!“) – drängen laufend neue Produkte auf den Markt. Und auch Verwaltungen und verwaltungsnahe Dienstleister wollen ihre Angebote in der neuen mobilen Welt von Tablets und ihren kleineren Geschwistern, den Smartphones, an den Mann bzw. an die Frau bringen. Bei den Nutzern der neuen mobilen Systeme streiten sich zwei Lager darum, ob es sich um eine eigenständige Kategorie von Geräten handelt, die vor allem den einfachen Zugang zu ansprechend aufbereiteten Inhalten immer und überall ermöglicht, oder ob diese doch nur etwas abgespeckte Bürocomputer sind, auf denen sich die tägliche Arbeit erledigen lassen muss – nur halt ein wenig eleganter. Auf jeden Fall machen sie die Lücke zwischen PDAs bzw. Smartphones einerseits und Arbeitsplatzrechnern und Notebooks andererseits kleiner. Entsprechend schwer fällt der Versuch, überhaupt eine Definition von „Tablet“ zu finden, die zum einen spezifisch genug ist, um diese Geräte von anderen Computern abzugrenzen, die zum anderen aber auch allgemein genug ist, um alle Spielarten der neuen Geräte zu erfassen. Daher werden im Folgenden einige charakteristische Eigenschaften dieser Geräte betrachtet.

Zunächst scheint das Tablet nur aus einem Bildschirm zu bestehen. Die Elektronik, die das Gerät zum Leben erweckt, ist direkt in das Gehäuse integriert. Da man in der Grundform eine Tastatur und andere Eingabegeräte vermisst, ist der Bildschirm zwecks Bedienung des Geräts als Touchscreen ausgelegt, auf dem man mit Stiften oder Fingern die Programme steuert. Zumeist sind sie auch gestenfähig, können also mit mehreren Fingern gleichzeitig bedient werden – etwa zum Vergrößern von angezeigten Objekten.

Die Geräte sollen kompakt und leicht sein, was bei ihrer vorwiegend mobilen Verwendung sinnvoll ist. Bei aktuellen Größen irgendwo zwischen DIN A5 und etwas kleiner als DIN A4 liegt es nahe, dass ihr Haupteinsatzgebiet nicht die Bearbeitung großer Rechentabellen oder die Programmierung komplexer Softwaresysteme in Entwicklungsumgebungen mit vielen Fenstern ist. Überhaupt gehört die Eingabe vieler Daten nicht unbedingt zu den bevorzugten Anwendungen, denn Tastatur oder Maus sind in der Regel stationäre Zusatzgeräte. Um dennoch Daten oder Text eingeben zu können, werden entweder Handschrifterkennung oder Bildschirmtastaturen angeboten. Folglich besteht der Anwendungszweck von Tablets eher im Konsum digitaler Medien. E-Books, Internetpublikationen und Videos können auf den Geräten betrachtet werden. Trotzdem gibt es neben den dafür geeigneten Programmen inzwischen eine Vielzahl von Apps für verschiedenste Zwecke: Zeichenprogramme, Bild- und Musikbearbeitung, spezielle Informationsdienste, Spiele u. v. m. In der Regel bilden diese Anwendungen mit der zugrundeliegenden Plattform aus Betriebssystem und Hardware eine mehr oder weniger stark verzahnte Einheit, da sie deren technische Spezifika stärker berücksichtigen müssen, als es bei standardisierten Rechnerplattformen der Fall ist. Das bedeutet für Anbieter von Anwendungen, dass sie sich indirekt für eine Hardwareplattform entscheiden müssen oder ihre Dienste für mehrere Plattformen entwickeln müssen, wenn sie diese für alle Geräte anbieten wollen.

Eng verknüpft mit verschiedenen Einsatzszenarien ist die Frage nach den Schnittstellen, die ein Tablet bieten soll. Geht man davon aus, dass das Tablet eher im Sinne eines erweiterten E-Book-Readers für den Medienkonsum bzw. für den Einsatz ähnlich eigenständiger Anwendungen konzipiert ist, wird man mit einem Minimum an Schnittstellen – bei Hard- und Software – auskommen. Betrachtet

man dagegen das Tablet als Allround-Arbeitsgerät, wird der Bedarf an Schnittstellen für Peripherie und Datenaustausch größer – z. B. für Netzwerk, USB-Hub, Tastatur, Bildschirm und Drucker. Allerdings können mehr Schnittstellen auch mit mehr Energie- und Platzbedarf sowie einer Gewichtszunahme des Gerätes verbunden sein. Bei den o. g. Größen und einem Gewicht von rund einem halben Kilogramm kommt es dann tatsächlich darauf an, was man wo machen möchte: in der S-Bahn stehend mit einer Hand das Gerät halten, um zu lesen, oder vorwiegend am Schreibtisch sitzend mit fester Unterlage und Peripheriegeräten, um „ernsthaft“ zu arbeiten. Derzeit definieren Tablets eine schicke eigenständige Geräteart zwischen Smartphone und Notebook bzw. Arbeitsplatzrechner. Ob sich dieses Nischenprofil weiter festigen wird oder ob diese Gattung sich in der einen oder anderen Richtung verschiebt, wird vielleicht schon die nächste Generation der Geräte zeigen. Das Tablet – dank ergänzter Telefonfunktion – am Ohr ist dabei genauso schwer vorstellbar wie ein Gerät, das eigentlich nur in der Docking-Station vernünftig zu gebrauchen ist.

Bewertung

Bei der Überlegung, ob Tablets in einer Verwaltung eingesetzt werden können oder sollen, spielen zwei Aspekte eine besondere Rolle. Zum einen ist das die Frage nach den Einsatzszenarien: Gibt es Anwendungsbereiche, in denen die Funktionen eines Tablets benötigt werden, ohne dass darüber hinausgehende Leistungen benötigt werden? Dies ist z. B. dann der Fall, wenn viele Akten und andere Sitzungsunterlagen abseits des normalen Büroarbeitsplatzes benötigt werden. Steht die mobile Bearbeitung von Dokumenten im Vordergrund, wird man eher zu einem mobilen Arbeitsplatzrechner tendieren, der auch weitere Aufgaben abdeckt. In diesem Fall wäre das Tablet dann ein Zusatzgerät mit Zusatzkosten. Diese Kosten sind aber derzeit noch durchaus nennenswert und wären für ein Zusatzgerät wohl nur in Ausnahmefällen zu rechtfertigen. Zum anderen ist die Frage nach der Sicherheit zu beantworten: Derzeit haben Tablets noch eher gerätespezifische Anwendungen und Betriebssysteme. Insbesondere letztere lassen sich in der Regel noch nicht austauschen – geschweige denn in verschiedenen Konfigurationen parallel betreiben. Es ist daher insbesondere zu klären, ob und ggf. wie solche Systeme mit angemessenem Aufwand in die IT-Sicherheitsarchitektur einer Verwaltung eingebunden werden können. Wenn – wie im Fall der hessischen Verwaltung geschehen – beide Fragen zufriedenstellend beantwortet werden können, können Tablets mehr sein als ein schickes „Spielzeug“ und ggf. die Beschaffung von Spezialgeräten überflüssig machen.

Verwaltungsrelevanz*:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

** für normalen Verwaltungsarbeitsplatz / für vorwiegend mobile Arbeit*

Graphén – der Stoff, aus dem die Träume sind

Schon bevor das Nobelpreiskomitee im Oktober 2010 bekannt gab, dass die Forschungsarbeiten von Andre Geim und Konstantin Novoselov zu dem modifizierten Kohlenstoff-Material mit dem begehrten Preis belohnt werden, kursierten Meldungen darüber, dass Graphén ein wahres Wunder an Werkstoff werden könne. Allein die Möglichkeit, die Ladezeit von Akkus durch Verwendung von Graphén-Elektroden von zwei Stunden auf zehn Minuten zu reduzieren, lässt manchen Mobilarbeiter ins Schwärmen geraten. Dabei denken Entwickler nicht nur an Kommunikationsgeräte, sondern auch an Elektrofahrzeuge. Ein schnelles Wiederaufladen der Akkus könnte die Akzeptanz solcher Fahrzeuge erhöhen.

Das Besondere an Graphén ist, dass daraus extrem dünne Schichten hergestellt werden können. Eine solche – nur ein Atom dicke – Schicht stellt

dann ein Material mit erstaunlichen Eigenschaften dar: Es leitet Strom besser als andere Materialien, ist innerhalb einer Kristallfläche nahezu so steif wie Diamant, durch die geringe Dicke der Materialschichten aber gleichzeitig flexibel und weist eine rd. 125-mal so große Zugfestigkeit auf wie Stahl. Damit scheint es ein Material zu sein, das dem bisher theoretischen Modell eines sog. Weltraumlifts Auftrieb geben könnte. Für die Informations- und Kommunikationstechnik interessanter sind aber die elektrischen Eigenschaften des Materials. Graphén wird als Nachfolger von Silicium bei der Herstellung von Transistoren gehandelt, da es Strom auch bei Zimmertemperatur besser leitet und wegen der geringen Dicke viel kleinere Schaltelemente ermöglicht. Dazu haben Prototypen solcher Transistoren schon Schaltfrequenzen von 100 GHz erreicht. Theoretisch soll noch die fünf- bis zehnfache Geschwindigkeit möglich sein, während Siliciumtransistoren bei fünf bis zehn GHz an ihre Grenzen stoßen.

Noch ist die Herstellung von Graphén aufwändig, da sehr dünne Schichten benötigt werden. Darüber hinaus dürfen die Schichten aber auch nicht beliebig breit sein und müssen „saubere“ Kanten aufweisen, da sonst die guten elektrischen Eigenschaften verloren gehen. Inzwischen ist es gelungen, ein Verfahren zu entwickeln, das zumindest im Labor reproduzierbar gute Ergebnisse bei der Herstellung einlagiger Graphén-Schichten liefert. Warum allerdings dieses Verfahren funktioniert, wissen die Forscher bisher noch nicht. Von der Grundlagenforschung bis zur massenhaften Produktion ist es also noch immer ein weiter Weg.

Bewertung

Noch befinden sich technische Entwicklungen auf Graphénbasis im Laborstadium oder sind reine Gedankenexperimente. Wenn der Werkstoff das hält, was er bisher verspricht, ist er einerseits dazu geeignet, die Miniaturisierung von Informations- und Kommunikationstechnik weiter deutlich voranzubringen. Andererseits könnten seine mechanischen Eigenschaften auch neue Anwendungsgebiete entstehen lassen. In der Verwaltungs-IT werden sich die Auswirkungen des neuen Werkstoffs zunächst nur mittelbar wahrnehmen lassen – nämlich durch die Miniaturisierung: Mehr Leistung auf kleinerer Fläche könnte sowohl die mobile Technik vereinfachen, als auch die stationäre Technik in Rechenzentren entlasten. Sofern die Forschungsergebnisse erfolgreich in Produkte am Markt umgesetzt werden können, wird die Technik wahrscheinlich sehr unauffällig in Büros und Serverräumen Einzug halten. Die Entwicklung ähnlich „wunderbarer“ Möglichkeiten in der Technik war auch schon den sog. Nanoröhrchen zugeschrieben worden. Diese sind aber nahezu aus der öffentlichen Wahrnehmung verschwunden. Wie die Entwicklung bei Graphén weitergeht, darf mit Spannung erwartet werden.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

BIOS ade? Jetzt kommt UEFI!

Für manche Nutzer von Computern ist es wichtig, auf ihrem Rechner mehrere Betriebssysteme nutzen zu können – z. B. eine Windows- und eine Linux-Variante. Und auch derjenige, der schon einmal beim Starten des Computers wichtige Einstellungen – wie die Reihenfolge der Geräte, von denen gebootet werden soll, – verändert hat, hat gemerkt, dass der Computer schon längst schwer beschäftigt ist, bevor das Betriebssystem seine Arbeit aufnimmt und bunte Logos oder gar eine Anmeldemaske auf den Bildschirm zaubert. Beteiligt an dieser Arbeit sind mehrere Komponenten: Sobald die Hardware mit Strom versorgt wird, startet die sog. Firmware – ein Programm, das in der Hardware des Computers fest installiert ist. Firmware findet sich aber auch in anderen „intelligenten“ elektronischen Geräten wie Digitalkameras, Haushaltsgeräten oder Handys.

Die Firmware umfasst mindestens alle diejenigen Programmroutinen, die nötig sind, um das Gerät in seinen Betriebszustand zu bringen. Bei Geräten, die über einen genau spezifizierten Funktionsumfang verfügen – z. B. ein DVD-Spieler oder eine Digitalkamera –, kann auch die komplette Anwendungssoftware Bestandteil der Firmware sein. Demgegenüber ist aber gerade der Zweck eines Computers, vielfältige und verschiedenartige Programme darauf nutzen zu können. Daher beschränkt sich die Firmware in der Regel darauf, grundlegende Hardwarekomponenten bereitzustellen und den Start eines Betriebssystems in die Wege zu leiten, das dann seinerseits die Softwaregrundlage für eine breite Palette von Anwendungsprogrammen ist. In den klassischen PCs übernimmt das sog. BIOS („basic input/output system“) diese Funktion. Doch dessen Funktionalität ließ sich zuletzt nur noch schwer an moderne Computerarchitekturen anpassen. Und so wurde insbesondere für den Einsatz auf 64-Bit-Systemen das Extensible Firmware Interface, EFI, spezifiziert, das das BIOS ersetzen soll. Durch die Beteiligung weiterer Hard- und Softwarehersteller wurde die Spezifikation bereits erweitert und wird nun unter der Bezeichnung Unified EFI, UEFI, weiterentwickelt.

Die Verbesserungen, die das Extensible Firmware Interface mit sich bringen soll, beziehen sich vorwiegend auf die systemnahen Komponenten von Hard- und Software und sind vom normalen PC-Nutzer nur bedingt wahrnehmbar. So können mit UEFI z. B. Gerätetreiber verwendet werden, die unabhängig vom Betriebssystem sind. Dies dürfte der Nutzer eher während seltener Installations- oder Wartungsarbeiten, aber weniger bei der täglichen Arbeit merken. Eher spürbar ist vielleicht eine Änderung, die es erlaubt, Festplattenpartitionen mit mehr als 2 TB Speicherkapazität zu nutzen bzw. von Platten entsprechender Größe zu booten. Zudem bringt UEFI ein eingebettetes Netzwerkmodul mit, das z. B. bei Fernwartung auf Systemebene genutzt werden kann. Dabei ist jedoch zu bedenken, dass ein solches eingebettetes Netzwerkmodul auch ein zusätzliches Sicherheitsrisiko darstellen kann, da es ggf. ohne die sonst üblichen Sicherheitsanwendungen verwendet werden kann, die erst nach dem Start eines Betriebssystems zur Verfügung stehen. Die größte Umstellung für Anwender dürfte UEFI aber dann bewirken, wenn Betriebssysteme nur noch ausschließlich auf diesem Standard aufsetzen. Zurzeit gibt es noch eine Reihe von Mechanismen, die es erlauben, Komponenten sowohl mit BIOS als auch mit UEFI zu nutzen. So wurde am Rande einer Präsentation zur kommenden Version des PC-Betriebssystems „Windows 8“ erwähnt, dass dieses System ausschließlich auf UEFI-Firmware laufen wird, jedoch nicht mit dem klassischen BIOS. Dadurch soll sich zwar der Bootvorgang beim Start des Computers auf wenige Sekunden reduzieren, allerdings wird für diesen Komfort dann häufig auch neue Hardware benötigt werden.

Ein Feature von UEFI, dessen Handhabung derzeit noch etwas umstritten ist, nennt sich „Secure Boot“. Dieses Protokoll sorgt dafür, dass nur mit akzeptierten, in der Firmware hinterlegten Schlüsseln signierte Programme oder Treiber installiert werden können. Da es keine allgemeine und unabhängige Stelle gibt, die derartige Schlüssel bereitstellt und verwaltet, hängt es von der Installation des Systems ab, ob und welche weiteren Anwendungen, Treiber oder alternative Betriebssysteme später noch installiert werden können.

Bewertung

Um unmittelbaren Einfluss auf die IT-Arbeit der Verwaltungen nehmen zu können, sitzt UEFI zu tief in der Rechnerarchitektur von Servern und Arbeitsplatzrechnern. Für den normalen Verwaltungsarbeitsplatz sollte die Funktionalität der Firmware transparent sein. Spürbare Änderungen werden eher über die Funktionen der Betriebssysteme vermittelt. Trotzdem sollten die aktuellen Entwicklungen auf dem Hard- und Softwaremarkt – letztere insbesondere im Hinblick auf die Betriebssysteme – sowie der „Secure Boot“-Thematik genau beobachtet werden, um rechtzeitig für notwendige Komponenten gerüstet zu sein, die auf Maschinen mit BIOS nicht mehr lauffähig sind. Dies kann erhebliche Auswirkungen auf notwendige Investitionen haben.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

LTE – Long Term Evolution

Mobile Kommunikation ist zu einem Geschäftsfeld geworden, das sich rasant entwickelt. Das wird spätestens dann deutlich, wenn man versucht, sich in den ganzen Kürzeln zurechtzufinden, die verschiedene Techniken oder Dienste des Mobilfunks bezeichnen. Die Einteilung der Standards in Generationen bringt ein wenig Struktur in das Wirrwarr, aber auch diese Zuordnung ist weniger eindeutig als man sich wünschen würde. Das wird auch bei der Technik deutlich, die derzeit eingeführt wird: Bei LTE, Long Term Evolution, hängt es vom Betrachter ab, ob dieser Standard schon zur vierten Generation, 4G, gezählt wird, oder ob er einer „Zwischengeneration", 3.9G, angehört.

Das augenscheinlichste Merkmal der Entwicklung von Mobilfunkstandards über die verschiedenen Generationen hinweg ist die Zunahme an Geschwindigkeit der Datenübertragung. Noch als vor einigen Jahren der Vorgänger von LTE – UMTS – eingeführt wurde, warteten zunächst viele Anwender und auch die Fachpresse auf die sog. Killerapplikation, die der schnellen Funkverbindung zum Durchbruch verhelfen sollte. Sie sollte die technische und auch finanzielle Notwendigkeit für so viel Leistung rechtfertigen und entsprechenden Nutzen stiften. Eine solche Anwendung hat es zwar nie gegeben, dennoch hat UMTS seinen Siegeszug angetreten und ist heute eine Standardtechnologie. Einen wesentlichen Beitrag dazu hat sicher das mobile Internet geleistet, das nun nicht mehr nur „grundsätzlich" verfügbar, sondern auch tatsächlich mit akzeptabler Geschwindigkeit nutzbar wurde. In Verbindung mit VPNs – also den abgesicherten Verbindungen in private Netze – ermöglichte UMTS auch erstmals die Nutzung komplexerer Firmenanwendungen für Mitarbeiter von Unternehmen, die auf Reisen oder bei Kunden waren. Doch so wie sich die Geschwindigkeit der Datenübertragung in leitungsgebundenen Netzen weiter erhöht, steigt auch der Geschwindigkeitshunger in den Funknetzen. Ob das daran liegt, dass mehr Fachdaten übertragen werden, oder die mobilen Anwendungen an sich mehr Kapazität beanspruchen, um sich optisch ansprechend und komfortabel bedienbar präsentieren zu können, ist dabei nachrangig. Bei den Nutzern mobiler Systeme – sei es auf Handys bzw. Smartphones oder Notebooks – herrscht der Anspruch vor, unterwegs nicht wesentlich schlechter ausgestattet zu sein als im Büro oder zuhause.

Neben der reinen verfügbaren Geschwindigkeit ist ein zweiter Faktor, der die Verbreitung von mobilen Diensten befördert hat, die Preisentwicklung. Zumindest dort, wo Personen oder Unternehmen von der elektronischen Mobilität profitieren, spricht man heutzutage kaum noch davon, dass UMTS zu teuer sei. Dank Flatrates zu akzeptablen Preisen entfällt die Notwendigkeit, jede einzelne Nutzung einer Funkverbindung begründen zu müssen.

Welche Perspektiven bietet nun aber der neue Mobilfunkstandard LTE? Er bringt zunächst einmal mehr Geschwindigkeit. Während UMTS Datenübertragung mit bis zu 384 kbit/s und seine Weiterentwicklung HSDPA (auch UMTS-Broadband) mit theoretisch bis zu rd. 14 Mbit/s ermöglichen, soll LTE Endgeräten erlauben, Daten mit bis zu 100 Mbit/s zu empfangen (sog. „Downlink") bzw. mit bis zu 50 Mbit/s zu senden (sog. „Uplink"). Durch sog. Multi-Carrier-Technik, bei der mehrere Übertragungskanäle gebündelt werden können, wurden in experimentellen Netzen sogar Übertragungsraten von 1,2 Gbit/s erreicht. Unter Live-Bedingungen – mit einem Empfänger in einem fahrenden Auto – wurden mit dieser „LTE Release 10" bzw. „LTE Advanced" genannten Technik beim Downlink immerhin noch 900 Mbit/s gemessen. Aber letzten Endes sind diese Werte nur theoretische Kenngrößen. Für den praktischen Einsatz werden deutlich geringere Raten erwartet, da sich in der Regel mehrere Nutzer die Übertragungs-

kanäle teilen müssen; hier werden 2Mbit/s als realistisch angesehen. Diese Effekte dürften insbesondere in zwei Einsatzszenarien auftreten: zum einen in Ballungszentren mit überdurchschnittlich vielen mobilen Nutzern und zum anderen dort, wo LTE den wesentlichen verfügbaren Zugang zum Breitbandnetz darstellt. In dünn besiedelten Gebieten, in denen die Erschließung mit Glasfaser oder auch konventionellen Kabeln zu aufwändig oder zu kostspielig wäre (➔ „FTTx – Glasfaser überall"), soll Mobilfunk die schnelle Anbindung gewährleisten. Ob diese Art der flächendeckenden Versorgung allerdings funktioniert, ist umstritten.

Zurzeit schießen die LTE-Netze – oder zumindest erste Netzknoten – wie die Pilze aus dem Boden. Aus allen Teilen Europas, Asiens und Nordamerikas werden Inbetriebnahmen und Aufbaupläne gemeldet – sei es der erste LTE-Sendemast in Deutschland (in Kyritz, Brandenburg), ein Netz in der als „weltweit anspruchsvollsten Region für Mobilfunk" titulierten Metropole Honkong oder die Vision eines flächendeckendes LTE-Netzes für die USA mit 40.000 Sendestationen. Neben experimentellen Netzen werden auch kommerzielle Installationen in der Presse bekanntgegeben. Und da der LTE-Standard verschiedene Parameter definiert, kann man des Öfteren vom „ersten kommerziellen LTE-Netz" lesen – mit bestimmten Nebenbedingungen. Eine dieser Nebenbedingungen kann das Frequenzband sein, in dem ein solches Netz arbeitet. Die für LTE vorgesehenen Frequenzbereiche liegen zwischen 800 MHz und 2,6 GHz. Dabei erlaubt LTE den Einsatz verschieden breiter Frequenzbänder von 1,25 MHz bis 20 MHz, wobei allerdings schmalere Kanäle zu Lasten der Übertragungsrate gehen.

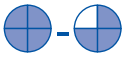
In Deutschland wurden die ersten Frequenzblöcke versteigert. Dabei sind die vergebenen Pakete mit der Auflage verbunden, zunächst unterversorgte Gebiete mit der neuen Technik zu versorgen. Dies gilt zumindest für die sog. digitale Dividende, also die Kanäle im 800 MHz-Bereich. Diese Frequenzen werden durch die zunehmende Digitalisierung des Rundfunks frei, da dieser deutlich weniger Bandbreite benötigt. Allerdings werden die entsprechenden Frequenzen nicht ausschließlich vom Rundfunk verwendet. Im Bereich um 850 MHz werden z. B. auch Geräte der Veranstaltungstechnik betrieben – etwa Funkmikrofone. Diese dürfen noch bis 2015 mit diesen Frequenzen betrieben werden, allerdings muss mit Störungen im Betrieb durch LTE gerechnet werden. Auch von möglichen Störungen des Fernsehempfangs per DVB-T oder des GPS-Empfangs durch LTE wird berichtet.

Bis die Herausforderungen und Chancen von LTE praktisch erprobt werden können, wird es aber noch etwas dauern. Endgeräte, die die neue Technik beherrschen, sind erst vereinzelt verfügbar. Neben LTE-Dongles, -Steckkarten für PCs und integrierten Lösungen, die seit Anfang 2011 langsam auf den Markt kommen, müssen vor allem noch entsprechende Handys entwickelt bzw. am Markt etabliert werden. Diese Zeit können die Netzbetreiber nutzen, um den Hauptteil der Arbeit beim Aufbau der Netze zu bewältigen. Der besteht nämlich weniger im Einrichten der einzelnen Sendestationen und deren Verbindung zum Betreibernetz über den sog. Backhaul, als vielmehr in der Prüfung aller Funktionalitäten und dem Finetuning der Konfigurationen zur Optimierung der Leistung. Auch geeignete Geschäftsmodelle müssen noch entwickelt werden, um die Nutzung von LTE für Endanwender attraktiv zu machen.

Bewertung

LTE kann verschiedene Auswirkungen auf die Verwaltungen haben: Zum einen kann dessen zunehmende technische Verfügbarkeit zu mehr Nachfrage von elektronischen Informations- und Dienstleistungen führen – sofern attraktivere Kostenmodelle für den schnellen Mobilfunk entwickelt werden. Insbesondere durch die verbesserte Versorgung in Gebieten, die bisher nicht über eine schnelle Internetanbindung verfügten, kann der Wunsch nach vollständig elektronisch abzuwickelnden E-Government-Verfahren wachsen: Wo der Behördengang eher eine Reise ist, wird eine solche Vereinfachung zunehmend nachgefragt werden. Ob LTE schließlich auch zu einer Weiterentwicklung von E-Government-Anwendungen beiträgt, erscheint fraglich, denn deren Komplexität ist i. d. R. eher strukturell bedingt und

lässt sich durch höhere Datenübertragungsraten nur bedingt in den Griff bekommen. Schließlich kann verbesserte Technik zu einer weiteren Mobilisierung und Flexibilisierung der Verwaltung beitragen, sofern organisatorische, rechtliche und finanzielle Rahmenbedingungen dies erlauben.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Höher, schneller, weiter – Wi-Fi entwickelt sich

Mobiles Arbeiten ist eines der ganz großen Themen – zumindest bei denen, die sich mit der Entwicklung von Arbeit und insbesondere dem Einsatz von IT beim Arbeiten befassen. Für viele beginnt dieses Thema aber schon in den eigenen vier Wänden – oder rundherum. Wer schnell noch eine E-Mail an seine Versicherung schreiben muss, oder Freunden ein paar Fotos vom letzten Ausflug schicken möchte, macht das oft lieber vom Balkon oder vom Sofa aus, als sich dafür an einen festen Arbeitsplatz am Schreibtisch zu setzen. Anstatt ein langes Netzkabel am Notebook hinter sich herzuschleifen, greift man dann gerne auf eine Funkverbindung mittels WLAN zurück. Auch bei vielen mobilen Endgeräten wie Smartphones, Mediaplayern und den neuen Tablets (➔ „Auf dem silbernen Tablet“) ist diese Technik vorhanden, so dass man mit ihnen Netzdienste auch ohne teuren Mobilfunktarif nutzen kann.

Mit der Wi-Fi-Alliance, die aus über 300 Firmen besteht, kümmert sich eine Organisation nicht nur um die Zertifizierung von Geräten nach den einschlägigen WLAN-Standards, um deren Funktionsfähigkeit sicherzustellen, sondern entwickelt auch eigene Spezifikationen. So sollen auf Basis dieser Standards neue Dienste und Einsatzmöglichkeiten entstehen. Eine der jüngsten Entwicklungen ist die Spezifikation für ein Peer-to-Peer-WLAN. Bei einem Peer-to-Peer-WLAN können – vergleichbar mit Bluetooth – Geräte direkt miteinander Verbindung aufnehmen, ohne über einen Access Point oder einen Router kommunizieren zu müssen. Dies funktioniert zwar auch heute schon grundsätzlich im sog. ad-hoc-Modus eines WLAN-Gerätes. Mit dem neuen Peer-to-Peer-Ansatz, Wi-Fi Direct genannt, sollen solche Verbindungen aber sicherer, einfacher einzurichten und leistungsfähiger sein, als es mit dem ad-hoc-Modus möglich ist. Zudem soll Wi-Fi Direct auch die Möglichkeit bieten, neben direkten Geräteverbindungen den Zugang zu einem typischen WLAN – im sog. Infrastruktur-Modus – zu nutzen. Dies ist im ad-hoc-Modus nicht möglich. Inzwischen sind eine ganze Reihe von Geräten mit der neuen Technik ausgestattet und zertifiziert worden. Deren Palette umfasst neben Wi-Fi-Adaptern, Smartphones und Medien-Servern auch insbesondere Bildschirme. Dabei werden Bildsignale auf einem Rechner komprimiert, der resultierende Datenstrom wird dann per WLAN an den Decoder des Monitors geschickt und dort wieder in Bildsignale umgewandelt. Diese Technik kommt vor allem in der Anbindung von Fernsehgeräten als Monitore für Medienrechner auch im Wohnzimmer zum Einsatz.

Neben der drahtlosen Verbindung zwischen Geräten ist die direkte Weitervermittlung der Daten von Endgeräten an Netzdienste ein Thema, das den Gedanken vom Netz der Dinge mit Leben erfüllt. Eine praktische, am Markt verfügbare Anwendung dieser direkten Verbindung ist das Weiterleiten von Fotos oder Videos – von der Kamera direkt ins Netz. Dazu werden Speicherkarten angeboten, die die Aufnahmen direkt verschicken können. Sofern die Kamera mit dem entsprechenden Format kompatibel ist, kann der Nutzer mehrere WLANs registrieren, in denen die Bilder vom Chip direkt übertragen werden sollen, wenn er sich in deren Reichweite befindet. Einige Kameras unterstützen diesen Automatismus, indem sie sich erst dann abschalten, wenn die Bilder übertragen sind. Sie bieten zum Teil auch spezielle Funktionen, mit denen man das Übertragen der Daten ein- und ausschalten kann.

Bilder lassen sich aber nicht nur auf den heimischen PC laden, sondern können auch direkt an Social Media- oder Fotodienste übertragen werden, sobald ein dafür geeigneter Hot Spot in der Nähe ist. Anhand von dessen Hot Spot-ID können die Bilder auch mit Ortsangaben versehen werden – sog. Geotagging. Für die direkte Verbindung der Speicherkarten sind alle Netze auf der Basis der Standards 802.11b und 802.11g sowie abwärtskompatible 802.11n-Netze geeignet.

Einige Kameramodelle können auch selber Bilder übertragen, ohne auf eine funkende Speicherkarte angewiesen zu sein. Auch sie senden auf Wunsch die Aufnahmen drahtlos an entsprechende Internetplattformen wie Flickr, facebook oder YouTube. Per E-Mail können dann Links auf die Bilder verschickt werden.

Alle diese neuen Anwendungsszenarien für WLAN-Technik beruhen – dem „local“ im Namen entsprechend – auf deren beschränkter Reichweite. Nach etwa 100 m werden die Wi-Fi-Signale handelsüblicher Technik auch bei freier Sicht so schwach, dass sie nicht mehr verlässlich nutzbar sind. Mit Spezialantennen lässt sich die Reichweite noch erhöhen, so dass man bis 300 m übertragen kann. Darüber hinaus werden aber Repeater benötigt, die das Signal aufnehmen und weitervermitteln. Beim Einsatz solcher technischen Zusatzgeräte und Hilfsmittel geht man in der Regel davon aus, dass die üblichen, großen Datenmengen moderner IuK-Geräte schnell übertragen werden sollen. Für Anwendungen, bei denen nur geringe Datenmengen übertragen werden müssen, lässt sich die Reichweite von Wi-Fi-Technik allerdings erheblich steigern. Mithilfe speziell entwickelter Algorithmen lassen sich so Wi-Fi-Signale noch in einer Entfernung von über 70 km bei freier Sicht empfangen. Die Technik könnte beim Aufbau von sog. „smart grids“ verwendet werden, also intelligenten Stromnetzen, in denen die Stromflüsse nach tatsächlichen Kapazitäten und nach tatsächlichem Verbrauch gesteuert werden. In einem 10.000 Quadratkilometer großen Versuchsgebiet konnten so die notwendigen Sensoren ihre Daten über nur 35 strategisch platzierte Access Points übermitteln. Mit konventioneller Funktechnik waren dazu über 1000 Access Points notwendig. Das Prinzip scheint also zu funktionieren. Ob und welche weiteren Anwendungsfälle dafür entwickelt werden, bleibt abzuwarten.

Einen anderen Weg zur Vergrößerung der Reichweite mit hohen Übertragungsraten schlägt Super-Wi-Fi ein: Dabei können über Entfernungen bis zu 100 km Übertragungsraten von bis zu 22 Mbit/s erreicht werden. Auch hier werden niedrigere Frequenzen verwendet als sonst bei Wi-Fi. Diese Frequenzen werden bei der Umstellung des Fernsehens von analoger auf digitale Technik frei. Der Ansatz von Super-Wi-Fi ähnelt damit dem des schnellen Mobilfunks LTE (➔ „LTE – Long Term Evolution“). Allerdings unterscheiden sich die Übertragungstechniken. Praktische Auswirkung hat das auf die Position von eingebundenen Geräten: Während sich diese bei Mobilfunktechnik innerhalb der Reichweite relativ frei bewegen können, müssen sie für Super-Wi-Fi vergleichsweise stationär betrieben werden und können ihre Position nur innerhalb enger Grenzen verändern. Auch die Betreibermodelle der beiden Techniken sollen sich unterscheiden: Während die Mobilfunkfrequenzen an kostenpflichtige Lizenzen gebunden sind, soll die Verwendung der Super-Wi-Fi-Frequenzen frei sein. Dies dürfte sich auch auf die Preise für Anwender auswirken.

Bewertung

Die aufgeführten Beispiele machen deutlich, dass die Art und Weise, wie WLAN-Technik genutzt wird, sich zu ändern beginnt. Noch zeigt sich dieser Wandel in sehr spezifischen Szenarien, in denen einerseits die Kommunikation zwischen Komponenten freier und flexibler wird und andererseits neue Anwendungsfelder für WLAN-Technik entstehen. Verwaltungsspezifische Anwendungen lassen sich derzeit noch nicht erkennen. Hier kann man ggf. von der allgemeinen Entwicklung profitieren. So können auch mobile Arbeitsplätze oder adhoc benötigte Netzwerke von den neuen Wi-Fi-Entwicklungen profitieren. Dabei muss aber in besonderem Maße darauf geachtet werden, welche Daten und Informationen in welcher Umgebung automatisch wohin

übermittelt werden. Spätestens wenn – z. B. im Rahmen einer mobilen Verwaltungsanwendung – personenbezogene Daten betroffen sind, darf eine drahtlose Übertragung nur in entsprechend abgesicherten Umgebungen erfolgen.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

FTTx – Glasfaser überall

Wenn es um die flächendeckende Versorgung der Bevölkerung mit schnellen Internetanschlüssen geht, denken viele zunächst an die Versorgung mit Funkverbindungen (➔ „LTE – Long Term Evolution“). Dabei ist die kabelgebundene Datenübertragung in puncto Geschwindigkeit der Funktechnik weit überlegen – zumindest wenn man dabei Glasfaserverbindungen betrachtet und nicht klassische Kupferkabel. Die technischen Möglichkeiten der Glasfaseranbindung bis in die Wohnung – engl. „fiber to the home“, FTTH, – scheinen nahezu unbegrenzt. Dass das Interesse an schnellen Funkverbindungen trotzdem so groß ist, ist insofern verständlich, als es einfacher ist, einen einzelnen Funkknoten neu zu installieren oder einen vorhandenen entsprechend umzurüsten, als Glasfaser für viele Einzelanschlüsse in die Fläche zu bringen. Dazu muss in der Regel eine komplett neue Infrastruktur errichtet werden, was mit erheblichen Investitionen seitens der Netzbetreiber verbunden ist. Diese Investitionen rentieren sich aber nur dann, wenn später genügend viele Haushalte die Anschlüsse tatsächlich nutzen und so eine entsprechende Marktabdeckung erreicht werden kann. Das wiederum ist dem Wettbewerb nicht zuträglich und kann damit die Endnutzerpreise in die Höhe treiben.

Die Frage nach der Wirtschaftlichkeit spielt also bei der Verbreitung von Glasfaserverbindungen bis zu den Endnutzern eine wesentliche Rolle. So wundert man sich nicht, zu lesen, dass die Gestaltung der Netzarchitektur eng mit dem angestrebten Geschäftsmodell verbunden ist und der Netzausbau einem „Endspiel in der Entwicklung der Telekommunikationsnetze“gleicht.

Dass für die Versorgung mit schnellen Glasfasernetzen bis in die Haushalte – zumindest in wesentlichen Teilen – eine neue Infrastruktur geschaffen werden muss, liegt daran, dass die Datenübertragung in der Glasfaser auf einem anderen physikalischen Prinzip beruht als bei Kupferkabeln: Hier fließen nicht Elektronen in Metallleitungen, sondern die Informationen werden per Licht übertragen, das durch nur Bruchteile von Millimetern dicke Glasfasern geleitet wird. Die Wirkung dieser Lichtleitung kennt man von Dekorationslampen, die in den 1960er/70er Jahren verbreitet waren: Ein Büschel flexible Glasfasern verteilte das Licht einer verborgenen Glühbirne am einen Ende zu winzigen Lichtpunkten am jeweils anderen Ende der Fasern. Bei den Lampen wie auch bei der Datenübertragung nutzt man aus, dass das Licht an den Rändern der einzelnen Fasern nahezu vollständig reflektiert wird und sich so entlang der Faserrichtung ohne nennenswerte Verluste ausbreiten kann. Dabei ist es durchaus möglich, die Fasern in einem gewissen Maß zu biegen, so dass Glasfaserkabel ähnlich wie elektrische Leitungen verlegt werden können.

Als Signalquellen können Laserdioden oder auch LEDs verwendet werden, die in der Lage sind, sehr kurze Lichtimpulse zu erzeugen. Da handelsübliche EDV-Geräte in der Regel nicht über einen optischen Eingang verfügen, sondern auf elektrische Signale angewiesen sind, müssen die Lichtsignale aus den Glasfasern zur weiteren Verarbeitung wieder in solche elektrischen Signale umgewandelt werden. Dies geschieht mit Hilfe von lichtempfindlichen Fotodioden. Wo diese Umsetzung geschieht – tatsächlich in der Wohnung, wie es der englische Begriff „fiber to the home“ impliziert, oder in einem von der Wohnung mehr oder weniger weit entfernten Verteiler – hat großen Einfluss auf die Ausgestaltung der In-

frastruktur und damit auch der Kosten und der Geschäftsmodelle. Je näher die Glasfaser bis an den Arbeitsplatz herangeführt wird – hier spricht man dann von „fiber to the desk“oder „fiber to the office“ – desto mehr Infrastruktur muss i. d. R. aufgebaut werden. Im Extremfall muss die komplette Verkabelung von den Verteilerknoten der Telekommunikationsanbieter bis zum Gebäude und auch die Gebäudeverkabelung auf Lichtwellenleiter umgestellt werden.

Entsprechend aller möglichen Zwischenstationen, an denen die Umsetzung zwischen optischer und elektrischer Datenübertragung erfolgen kann, spricht man dann auch von „fiber to the ...“

neighborhood / node	Nachbarschaft resp. (Verteil-)Knoten	FTTN
curb	Bordstein, Straßenrand	FTTC
premise	(Firmen-)Gelände, Liegenschaft	FTTP
building	Gebäude(-verteiler)	FTTB
enclosure	Verteilerschrank (z. B. Stockwerk)	FTTE

Diese – und weitere sehr fein abgestufte – Modelle entscheiden auch darüber, wo sich die technischen Komponenten befinden, die für die Umsetzung der Datenströme zwischen den Weitverkehrsnetzen und den lokalen Versorgungsnetzen befinden. Da die Komponenten der Glasfasernetze i. d. R. dem Netzanbieter gehören, entstehen hier evtl. Abhängigkeiten zwischen den Anbietern und Nutzern, die – wie weiter oben gesagt – dem Wettbewerb abträglich sind. Daher muss ggf. durch regulierende Maßnahmen dafür gesorgt werden, dass die physikalischen Netze auch für andere Anbieter geöffnet werden.

Neben den Kosten zur Realisierung der gewählten Topologie haben weitere Parameter in den verschiedenen Modellen Einfluss darauf, welche Leistung der Endnutzer schließlich an seinem Arbeitsplatz abrufen kann. So hängen zum Beispiel die Geschwindigkeiten für Down- und für Upload von der eingesetzten Technik ab. Hier werden je nach Modell 100 MBit/s bis rd. 2,5 GBit/s für die Teilnehmer erreicht.

So vielfältig wie die technischen Möglichkeiten sind auch die verschiedenen Initiativen der Wirtschaft und der Politik zur Verbreitung flächendeckender Glasfaserverbindungen. Während einige Anbieter verschiedene lokale bzw. regionale Pilotmodelle mit einigen Tausend Teilnehmern realisiert haben, wird auf nationaler und internationaler Ebene an der Mindestversorgung gearbeitet. Dabei reicht das Spektrum der angestrebten Leistungen von 2 MBit/s für jeden Einwohner in Großbritannien bis zu 1 GBit/s landesweit in Südkorea. Die vergleichsweise hochgesteckten Ziele in asiatischen Staaten lassen sich darin erklären, dass dort DSL schon seit Jahren eine Auslauftechnik ist, die von Glasfasertechniken abgelöst wird, während die „kupfergebundene“ Technik in einigen westlichen Staaten noch weiterhin auf- und ausgebaut wird. So sollen in Japan bereits über 14 Millionen FTTH/FTTB-Anschlüsse realisiert sein. In Deutschland wird angestrebt, dass 75 % der Haushalte bis 2014 mit mind. 50 MBit/s versorgt werden können. Auch das Land Hessen hat sich bezüglich der Versorgung mit schnellen Internetzugängen diesem Ziel angeschlossen. In seiner Strategie für „Next Generation Access“, NGA-Strategie, setzt das Land auf FTTH, also die flächendeckende Verfügbarkeit von Glasfaser bis zur Wohnung, ergänzt um hochbitratige Mobilfunkversorgung. Die Komplexität eines solchen Unterfangens wird deutlich, wenn man sich die Rolle des Landes ansieht: Auch wenn man sich hier im Kern auf die Förderung der Anschlussbemühungen und auf die Vermittlung zwischen den Beteiligten konzentriert, sind bei den konkreten Maßnahmen die Interessen von Netzanbietern, Unternehmen, Bürgern, Kommunen und Weiteren in Einklang zu bringen – und zwar unter Berücksichtigung entsprechender Initiativen auf Bundes- und auf EU-Ebene.

Bewertung

Die öffentlichen Verwaltungen sind auf vielfache Weise in den Auf- und Ausbau flächendeckender Glasfaserangebote sowie schneller Mobilfunktechniken eingebunden. Das ist schon deshalb erforderlich, weil die Interessen sowie Erfordernisse potenzieller Nutzer einerseits und der – i. d. R. privatwirtschaftlichen – Anbieter andererseits nicht immer übereinstimmen. Das gilt insbesondere dann, wenn es um die Versorgung gering besiedelter Gebiete geht.

Aber auch als Nutzer kann die Verwaltung von der Ausweitung von FTTH-Angeboten profitieren, da so auch Dienststellen außerhalb der Ballungszentren adäquat versorgt werden können. Dies spielt insbesondere dann eine Rolle, wenn Anwendungen aus einer Datenzentrale oder gar von einer anderen, weit entfernten Gebietskörperschaft genutzt werden sollen.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Licht aus – Spot an zur Datenübertragung

Fast überall, wo wir uns bewegen, werden Daten übertragen – per Glasfaser oder Kupferkabel, per Satellit, Mobilfunk, WLAN, Bluetooth oder mit anderen Techniken. Gerade die drahtlosen Möglichkeiten der Übertragung sind sowohl für Dienstbetreiber als auch für Dienstnutzer sehr attraktiv, da sie leichte Anpassungen an veränderte Bedingungen wie die Standorte von Geräten erlauben, ohne dass dabei neue Kabel verlegt werden müssen. Auch im Büro oder in der Wohnung helfen solche Techniken das Kabelgewirr auf dem Schreibtisch zu verringern. Und bei Konferenzen oder ähnlichen Veranstaltungen reduziert sich das Verkabelungsproblem durch Funktechniken auf die Stromversorgung.

Doch nicht überall sind Funknetze erlaubt oder erwünscht. Z. B. soll in Krankenhäusern vermieden werden, dass medizintechnische Geräte durch Funkverbindungen gestört werden. Und so wird nach weiteren Alternativen geforscht. Eine neue Technik, die dabei entwickelt wurde, nutzt sichtbares Licht für die hochfrequente Datenübertragung. Mit Raten von bis zu 500 MBit/s kann diese Technik heute durchaus als schnell bezeichnet werden. Möglich wird dies durch den Einsatz von LEDs, die mit sehr schnellen Schaltvorgängen die notwendige Zahl von Lichtimpulsen erzeugen können, um auf nennenswerte Datenraten zu kommen. Für einen ggf. anwesenden Nutzer sind diese Lichtblitze nicht wahrnehmbar. Das menschliche Auge vermag nur etwa 25 Einzelbilder in der Sekunde zu unterscheiden. Weniger Bilder führen zu einem Flackern. Mehr Bildimpulse verschmelzen miteinander, so dass schon das – verglichen mit der eingesetzten LED-Technik langsame – Ein- und Ausschalten einer Glühbirne durch das normale 50 Hz-Wechselstromnetz nicht mehr wahrgenommen wird.

Die Fotodiode im Empfänger des Licht-Daten-Stroms ist weniger träge als das menschliche Auge. Sie kann die einzelnen Lichtsignale wieder in elektrische Impulse verwandeln, die dann von einem Computer aufgenommen werden können.

Die schnellen Übertragungsraten sind derzeit noch an einige Rahmenbedingungen geknüpft, die den praktischen Einsatz einschränken: Die Verwendung von sichtbarem Licht bedingt eine direkte und ungehinderte Sicht zwischen Sender und Empfänger, die beide aufeinander ausgerichtet sein müssen. Dies verhindert zwar das Abhören des Datenstroms, da ein Lauschangriff nur entlang der optischen Verbindung möglich wäre, bedingt aber auch eine stabile Installation von Sender und Empfänger. Für beliebig in einem Konferenzraum aufgestellte Notebooks ließe sich also kaum eine brauchbare Anwendung realisieren. Zudem verläuft der Datenstrom in einer Einbahnstraße – von einem definierten Sender zu einem ausgemachten Empfänger. Eine Internetverbindung z. B. lässt sich auf diese einfache Weise nicht realisieren, da sie eine wechselseitige Kommunikation – Absetzen eines HTTP-Requests und Empfangen der Antwort – nicht ohne Weiteres ermöglicht.

Die Forscher vermuten, dass sich mit unsichtbarem Infrarotlicht die wechselseitige Kommunikation eher realisieren lässt. Einfache und langsame technische Realisierungen gibt es bereits seit geraumer Zeit für die Kommunikation zwischen einzelnen Geräten wie PC und Drucker. Hierbei ist auch die Positionierung von Sender und Empfänger zueinander weniger kritisch, da auch im Raum reflektiertes Licht zur Datenübertragung genutzt werden könnte. Dadurch muss nicht unbedingt direkte Sichtverbindung bestehen. Allerdings sinkt dabei auch die Datenübertragungsrate – hier werden zunächst 100 Mbit/s angestrebt. Immerhin wäre dann die Infrarottechnik immer noch eine gute Alternative zu bestehenden WLANs. Da diese Funknetze auch über optische Grenzen – wie z. B. Wände – hinweg genutzt werden können, sind sie zwar sehr beliebt. Innerhalb von Gebäuden kann es aber vorkommen, dass sie sich gegenseitig stören. Hier könnten „optische Netze“ ggf. zu einer Trennung der Datenströme beitragen.

Bewertung

Die schnelle Datenübertragung per Licht befindet sich noch im Forschungsstadium. Bisher zeichnen sich nur sehr spezifische Anwendungen in relativ starr aufgebauten Systemen ab: Die Kommunikation verläuft im Wesentlichen in eine Richtung und die empfangenden Geräte befinden sich an klar definierten Positionen. Dies kennzeichnet eher einen produzierenden Betrieb, in dem z. B. Maschinen Instruktionen empfangen, als ein klassisches Verwaltungsumfeld, in dem Fachverfahren in der Regel bidirektional kommunizieren. In der Verwaltung wird für den Einsatz von Licht als kabelloser Datenträger entscheidend sein, ob die räumliche Flexibilisierung der Technik mit entsprechenden Übertragungsraten klassische Netztechniken tatsächlich überholen kann.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

IT-Sicherheit

Ich weiß, was du letzte Woche gelesen hast! – History Stealing

Es kann den Internetnutzer schon manchmal gruseln, wenn er beim Stöbern im Netz plötzlich auf einer Webseite passende Werbung zu einem Thema angezeigt bekommt, das er vor kurzem an anderer Stelle recherchiert hat. Der erste Verdacht richtet sich in solchen Fällen oft gegen sog. Cookies, kleine Informationsschnipsel, die eine Webseite auf dem Computer ablegen und ggf. später wieder abfragen kann. Doch selbst wenn die Verwendung von Cookies im Browser deaktiviert ist, können Informationen über aufgesuchte Webseiten in unbefugte Hände – oder besser: Systeme – gelangen. Ein Ansatzpunkt dafür kann die Chronik oder „History“ sein, in der der Browser die Adressen der zuletzt besuchten Seiten ablegt. Dieses Verzeichnis ist für den regulären Nutzer dann praktisch, wenn er eine Seite nochmal aufsuchen möchte, deren genaue URL er sich nicht gemerkt hat. Doch diese Liste kann auch von fremden Webseiten dazu genutzt werden, zu ermitteln, welche Seiten besucht wurden. Dies geschieht zwar nicht durch direktes Auslesen der Daten, es gibt aber Möglichkeiten, gezielt abzufragen, ob bestimmte Seiten in der Chronik enthalten sind. Diese Technik des Schnüffelns (engl. „history sniffing“) oder des Ermittelns (engl. „history detection“) in der Chronik macht sich zunutze, dass aus Gründen der besseren Handhabbarkeit von Webangeboten die Links auf bereits besuchte Seiten anders dargestellt werden können als diejenigen auf noch ungelesene Seiten. Traditionell werden neue Links blau, bereits benutzte Links rot dargestellt. Aber auch andere Farben und weitere Attribute sind zur Unterscheidung einsetzbar. Möchte nun ein Angreifer herausfinden, ob der Besucher seiner Seite eine bestimmte Webadresse schon einmal aufgerufen hat, so kann er einen für den Nutzer verborgenen Link auf diese Webadresse in seine Seite einbauen. Durch entsprechende Abfragen – z. B. durch eine JavaScript-Funktion – kann er dann ermitteln, ob die Webadresse mit den Attributen für neue oder für bereits gelesene Seiten versehen ist. Diese Abfrage findet aber auf dem Computer des ahnungslosen Nutzers statt. Damit der Angreifer diese Information auch verwenden kann, muss er seine eigene Seite so präparieren, dass sie die Information an ihn übermittelt. Dazu wird die URL der ermittelten Seite in die Webadresse eines Phantasieobjektes – z. B. eines Bildes – eingebaut, das eine weitere JavaScript-Funktion anschließend dynamisch vom Server des Angreifers nachzuladen versucht. Das wird zwar zu keinem Resultat führen, da ein Objekt dieses Namens nicht existiert. Aber nun hat der Angreifer die Information über die früher betrachtete Webadresse auf seinem Server. Diese Technik lässt sich so weit verfeinern, dass sich neben einfachen Webadressen auch Parameter von Suchabfragen, Postleitzahlen oder aktuell gelesene Nachrichten ermitteln lassen. Durch das Abfragen von vielen – i. d. R. populären – Webadressen und ggf. Parametern lässt sich so ein recht gutes Abbild der Browserchronik ermitteln und übertragen – sog. „history stealing“. Somit verfügt der Angreifer über ein Nutzerprofil der ausgespähten Person.

Gegen diese Art des Angriffs hilft es, JavaScript im Browser zu deaktivieren. Es gibt aber auch Varianten dieser Angriffstechnik, die ohne JavaScript auskommen. Dabei werden z. B. über Stylesheets spezifische Grafiken zur Gestaltung von besuchten bzw. neuen Links eingesetzt. Indem analysiert wird, welche Grafiken verwendet werden, können ebenfalls Profile vom Surfverhalten des Nutzers erstellt werden.

Der Nutzen von „history sniffing“ oder „history stealing“ besteht für den Angreifer nicht allein darin, gezielt Werbung für Webseiten einzublenden, die den Nutzer vermutlich interessieren. Die übermittelten Informationen lassen sich auch dazu verwenden, dem Websurfer eine gefälschte Seite eines von ihm genutzten Dienstes unterzuschieben: Wenn der Angreifer weiß, dass der Nutzer z. B. Kunde eines bestimmten Webmail-Dienstes ist, kann er eine fingierte Anmeldeseite dieses Dienstes darstellen, um die Daten des Nutzerkontos zu stehlen. Die Darstellung einer solchen Seite kann z. B. ganz diskret im Hintergrund auf einer nicht sichtbaren Registerseite (engl. „tab“) des Browsers erfolgen.

Eine weitere Anwendung für die Technik „history stealing“ geschieht im Rahmen des sog. „history caching“. Hier wird die Browserchronik dazu ver-

wendet, den Link auf ein sog. Zombie-Cookie abzulegen. Während die eigentliche Cookie-Information auf einem fremden Server abgelegt wird, wird eine Referenz auf diese Information wieder mittels unsichtbarem Link in der Chronik abgelegt. Die Referenz in der Chronik kann bei späteren Besuchen der Angreiferseite wiederum mit den beschriebenen Techniken abgefragt werden. Durch die Kombination mit weiteren Techniken erlaubt es diese Art des Angriffs Cookies zu erstellen, die nur sehr schwierig zu löschen sind.

Was sich liest wie komplizierte Experimente aus dem Web-Labor, ist tatsächlich ein Massenphänomen. In einer breit angelegten Untersuchung wurde ermittelt, dass von rd. 270.000 Teilnehmern an einem Test etwa 76 % durch „history stealing“ gefährdet waren. Eine Analyse von 50.000 populären Websites ergab, dass knapp 500 davon die Eigenschaften von gelesenen bzw. neuen Links auswerteten, und knapp 50 davon übermittelten Chronikinformationen an ihren Server. Eine genauere Untersuchung ergab weiterhin, dass in den meisten dieser Fälle beim „history stealing“ fertige Codebibliotheken zur Anwendung kamen. Auch wenn diese Zahlen absolut gesehen klein sind, zeigen sie doch, dass „history stealing“ – bezogen auf die Masse der Webseiten im Internet – eine ernstzunehmende Technik zur Erstellung von Nutzerprofilen ist.

Abwehrtechniken gegen diese Angriffe sind schwierig zu entwickeln, da die Angriffstechniken Merkmale von Webseiten bzw. Browsern ausnutzen, die aus Gründen der besseren Handhabbarkeit eigentlich gewollt sind. So ist es nicht verwunderlich, dass die Diskussion um eine konkrete Lösung für einen einzelnen Webbrowser mehrere Jahre dauerte.

Bewertung

Sowohl Kunden als auch Mitarbeiter von Verwaltungen können Ziele von „history stealing“ sein. So ließen sich z. B. Informationen sammeln, welche Firmen sich auf einer Vergabeplattform bewegen – und evtl. an welchen Verfahren sie sich evtl. beteiligen. Umgekehrt können Informationen darüber gesammelt werden, welche Fachthemen und Dienstleistungen für Verwaltungen oder Politik interessant sind. Dadurch kann ggf. Einfluss auf entsprechende Vorhaben genommen werden. Solange nicht tatsächlich effektive Abwehrtechniken gegen Angriffe über die Browserchronik entwickelt werden, dürfte eine Sensibilisierung der Anwender für das Thema der beste Schutz vor möglichen Schäden sein.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit*:	

** Einfache Abwehrmaßnahmen wie das regelmäßige Löschen der Browserchronik oder das gesicherte Surfen lassen sich sofort umsetzen. Technische Lösungen sind aus den genannten Gründen nicht in Sicht.*

Mit den eigenen Waffen – Kryptovirologie und Kleptografie

Wenn man einen Einbruch in einem Haus bemerkt, ist das Vorkommnis oft beunruhigend und der entdeckte Schaden groß. Noch unangenehmer ist es aber, wenn der Dieb sich seine eigene, verborgene Hintertür einbaut, zu der nur er einen Spezialschlüssel hat. Er kann über längere Zeit immer wieder kleinere Schäden anrichten, ohne dass das direkt auffällt. Auch in der IT gibt es Szenarien, in denen Angriffe auf Daten stattfinden, die zunächst unbemerkt erfolgen und bei denen – sofern sie doch entdeckt werden – der Urheber kaum zu entdecken ist. Möglich wird das dadurch, dass hierbei Kryptografie verwendet wird, um die Spuren der Angriffstechnik zu verbergen. So werden Mechanismen, die eigentlich zum Schutz von Daten geschaffen wurden, als Waffe gegen diese Daten bzw. deren Besitzer eingesetzt.

Ein solches Szenario ist die „Online Erpressung“. Hierbei werden Daten auf dem System ihres Besitzers verschlüsselt und erst nach Zahlung von Lösegeld – oder Weitergabe der Daten – wieder entschlüsselt. Dazu erstellt der Angreifer zunächst einen starken asymmetrischen Schlüssel – also ein Paar, bestehend aus einem öffentlichen und einem privaten Schlüssel. Der öffentliche Schlüssel wird in einen Virus eingebaut, der auf die Zielmaschine gelangen muss. Dort erzeugt der Virus einen symmetrischen Schlüssel, mit dem er die dortigen Daten verschlüsselt. Anschließend wird der gerade verwendete, symmetrische Schlüssel mit dem öffentlichen Schlüssel des Angreifers verschlüsselt, den der Virus ja mitgebracht hatte. Die ursprünglichen Daten und der „Klartext“ des symmetrischen Schlüssels werden dann gelöscht. Nun befinden sich auf dem angegriffenen Rechner nur noch die verschlüsselten Daten, der verschlüsselte symmetrische Schlüssel und der öffentliche Schlüssel des Angreifers. Um wieder an die ursprünglichen Daten zu kommen, müsste der symmetrische Schlüssel wiederhergestellt werden. Dazu ist aber der private Schlüssel des asymmetrischen Paares erforderlich, der jedoch ausschließlich beim Angreifer verblieben ist. Der Virus kann nun den Besitzer der Daten über die „Entführung“ der Daten informieren und darauf hinweisen, dass er gegen Zahlung eines Lösegeldes und nach Übermittlung des verschlüsselten symmetrischen Schlüssels den Klartext des symmetrischen Schlüssels erhält, mit dem er seine Daten wieder restaurieren kann. Anstelle eines Lösegeldes kann auch die Herausgabe der (verschlüsselten) Daten selber erpresst werden, so dass der Angreifer bei der Entschlüsselung der Daten auch an Geschäftsgeheimnisse gelangen kann.

Sofern die Wege zur Übermittlung von Geld bzw. Informationen an den Angreifer nicht nachverfolgt werden können, ist diese Technik für den Angreifer relativ sicher: Zum einen gibt es keinen Hinweis auf den privaten Schlüssel, selbst wenn der Virus analysiert werden kann. Zum anderen existiert der symmetrische Schlüssel nur kurze Zeit während des Codiervorgangs und wird als Klartext nicht dauerhaft gespeichert. Wenn dann von den ursprünglichen Daten nicht ein aktuelles und unversehrtes Backup existiert, ist deren Eigentümer bei einem erfolgreichen Angriff dem Erpresser hilflos ausgeliefert.

Verschlüsselung lässt sich auch einsetzen, um unbemerkt Login-Namen und Passwörter zu stehlen. Bei einem Diebstahl mit Hilfe eines klassischen Trojaners besteht die Gefahr, dass der Dieb auf frischer Tat ertappt wird und die gestohlenen Daten bei sich hat. Auch die Übermittlung der gestohlenen Login-Daten lässt sich ggf. recht einfach feststellen, indem z. B. der Datenverkehr auf die Klartexte der Informationen überprüft wird.

Um diese Gefahren der Entdeckung zu verringern, können die Daten zusätzlich asymmetrisch verschlüsselt und anschließend relativ weit verbreitet werden – z. B. mithilfe modifizierter Dateien. So hat der Angreifer die Chance, unauffällig an die gestohlenen Informationen zu gelangen, ohne den evtl. besonders überwachten Zielrechner benutzen zu müssen. Fällt trotzdem ein Verdacht auf ihn, weiß er nichts davon, was er da für merkwürdige – weil verschlüsselte – Informationen erhalten hat. Und nur er kann mit seinem privaten Schlüssel die echten Login-Daten wieder verfügbar machen.

Diese Beispiele von sog. Kryptovirologie zeigen, wie mithilfe von Kryptotechniken, die eigentlich zur

Sicherheit von Daten beitragen sollen, Schadprogramme „verbessert“ und Angriffe gestartet werden können.

Eine Stufe weiter geht die sog. Kleptografie, bei der Kombinationen von Kryptotechniken und Schadsoftware dazu eingesetzt werden, ihrerseits Sicherheitskomponenten zu kompromittieren. Dazu wurden bereits verschiedene Verfahren beschrieben, mit deren Hilfe sich die Erzeugung von Codierungsschlüsseln so manipulieren lässt, dass der Angreifer die vermeintlich sicheren Schlüssel brechen kann. Ein Ansatzpunkt sind dabei die Zufallszahlen, die in der Regel verwendet werden, um Schlüssel zu erzeugen. Verwendet man anstelle echter Zufallszahlen sog. Pseudozufallszahlen, die zwar willkürlich aussehen, tatsächlich aber nach einem festen Algorithmus und mit einem definierten Startwert gebildet werden, lassen sich auch die daraus abgeleiteten Schlüssel rekonstruieren. Weitergehende Manipulationen bestehen z. B. darin, Informationen über die erzeugten Schlüssel in deren öffentlichen Teilen zu verstecken – und zwar selber wieder mit dem Schlüssel des Angreifers codiert.

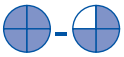
Solche Manipulationen von Sicherheitskomponenten profitieren ggf. davon, dass sie in der Regel gekapselt sind und z. B. der Quellcode der tatsächlichen Implementierung nicht bekannt ist. Und selbst wenn die Algorithmen offen liegen, ist die tatsächliche Funktion einer konkreten Sicherheitskomponente nur durch sog. Black Box-Testen zu überprüfen.

Für den normalen Anwender – auch im professionellen Umfeld – mögen die beschriebenen Techniken eher als Gedankenexperimente oder Ergebnisse von Laboruntersuchungen erscheinen. Und auch wenn ihre Anwendung an weitere Rahmenbedingungen gebunden ist – z. B. dass ein Virus tatsächlich den Zielrechner erreicht oder dass dort Zugriff auf benötigte Funktionen besteht – machen sie aber zumindest deutlich, dass das Vertrauen in Sicherheitsfunktionen gut begründet sein muss. Gerade im Zusammenhang mit Stichworten wie „trusted computing“ oder „trusted cloud“ sollten Anwender sich die Mühe machen, genau hinter die Technik und Geschäftsbedingungen zu schauen, bevor sie sich auf vermeintliche Sicherheit verlassen. So werden zwar beim „trusted computing“ auch Kryptoverfahren eingesetzt, um den Betrieb abzusichern bzw. verlässlicher zu machen. Hier geht es jedoch eher darum, die Integrität von Hard- und Software gegenüber Lieferanten abzusichern und diesen ggf. Eingriffe in das System zu ermöglichen, als für den Anwender eine vertrauenswürdige (engl. „trustworthy“) Betriebsumgebung zu schaffen. Und auch beim Cloud Computing ist das Sicherheitsetikett von potenziellen Lösungen kritisch zu prüfen, bevor Unternehmen oder Verwaltungen ihre Daten Dritten übergeben. In der jüngeren Vergangenheit gab es Meldungen darüber, dass Cloud-Anbieter fremden Geheimdiensten Zugriff auf Daten eingeräumt haben, die außerhalb ihres Zuständigkeitsgebietes – z. B. in Deutschland – gespeichert waren. Wenn man dann damit rechnen muss, dass die zum Schutz der eigenen Daten eingesetzten Kryptokomponenten ebenfalls Hintertüren enthalten, nimmt das Vertrauen in Sicherheit schnell Schaden. Eine Möglichkeit, die resultierenden Risiken zu reduzieren, besteht z. B. darin, verschiedene Sicherheitskomponenten von tatsächlich voneinander unabhängigen Lieferanten zu beziehen. Trotz möglicher Gegenmaßnahmen wird das Thema Verlässlichkeit und Vertrauenswürdigkeit von fertigen Produkten und Diensten aber mit deren zunehmender Funktionalität und Komplexität an Bedeutung gewinnen.

Bewertung

Auch für Verwaltungen und Regierungen sind Angriffe auf ihre Rechnersysteme von hoher Bedeutung. Insbesondere, wenn es dem Angreifer nicht um schnelle spektakuläre Erfolge geht, sondern er mehr Wert auf dauerhaften Zugriff auf Daten legt, sind für ihn die durch Verschlüsselung verborgenen Methoden in vermeintlich sicheren Umgebungen das Mittel der Wahl. Es ist daher wichtig, dass die Angriffsmethoden bei den Anbietern öffentlicher IT-Dienstleistungen bekannt sind und die Entwicklung von Gegenmaßnahmen begleitet wird. Neben der Sensibilisierung aller Mitarbeiter ist es einmal mehr eine Grundvoraussetzung für Sicherheit, dass die vorhandenen Sicherheitsmaßnahmen – auch im

Hinblick auf die Verfügbarkeit von Daten – konsequent umgesetzt und ggf. auf den Stand der Technik gebracht werden. Die gute technische Vernetzung der verschiedenen Verwaltungen, die evtl. neue Einfallwege für verborgene Schadprogramme eröffnet, sollte sich noch mehr in der organisatorischen Vernetzung bei der Abwehr derartiger Angriffe widerspiegeln.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Secure by design – für die innere Sicherheit

„Nichts ist sicher!“ möchte man angesichts täglich neuer Meldungen über Datenverluste und sog. Cyber-Attacken sagen – zumindest in Bezug auf die Informationstechnik. Dabei beziehen sich die wenigsten dieser Meldungen auf „Pannen“ – also relativ zufällige sicherheitsrelevante Ereignisse –, sondern vielmehr auf gezielte Angriffe auf Netze, Rechnersysteme und Anwendungen. Die Sicherheitsmodelle, die auf Risikobetrachtungen mit Eintrittswahrscheinlichkeiten für Bedrohungen basieren, bilden daher nur noch einen Teil der Wirklichkeit ab. Solche Überlegungen sind auf sporadische Ausfälle technischer Komponenten, auf vereinzelte Fehlbedienungen oder Datenfehler anwendbar. Wenn man aber ins Kalkül nimmt, dass ein Informationssystem das ausgesuchte Ziel eines bewusst durchgeführten Angriffs wird, passen solche Modelle nicht mehr. Erschwert wird die klassische Risikobetrachtung dadurch, dass es zahlreiche mögliche Angriffspunkte gibt – z. B. Datenverkehr, Speichersysteme, Datenbanken oder Benutzeroberflächen – und für manche Angriffstechniken inzwischen Rechenleistung in großen Mengen zur Verfügung steht. Dazu können sich Angreifer der Computer ansonsten unbeteiligter Personen bedienen, indem sie z. B. sog. Bot-Netze aufbauen, oder sie kaufen Rechenleistung bei Cloud-Anbietern, um „brute force“-Angriffe auf Verschlüsselungssysteme durchzuführen. Ist das Ziel des Angreifers nicht der schnelle Erfolg, sondern eher der längerfristige Zugriff auf Informationssysteme, können Angriffe auch über längere Zeit und dafür mit weniger einzelnen Interaktionen erfolgen, wodurch sie schwieriger zu entdecken sind. So hat ein Hersteller von IT-Sicherheitskomponenten gerade ermittelt, dass über mehrere Jahre hinweg IT-Systeme von mehr als 70 Regierungen, Firmen und internationalen Organisationen in einer umfassenden Angriffsserie ausspioniert wurden – zum Teil über viele Monate hinweg.

Klassische Abwehrmaßnahmen gegen solche Angriffe von außen – und auch innerhalb einer Organisation – schließen u. a. Firewalls, Verschlüsselungsmechanismen, Zugangsbeschränkungen, Intrusion-Detection-Systeme und Penetrationstests ein. Daher kann großer Schaden entstehen, wenn derartige Schutzmechanismen überwunden werden und Angreifer sich innerhalb von Systemgrenzen relativ frei bewegen können, denn von dort aus erreichbare Anwendungen verfügen oft über geringere Schutzmechanismen bzw. sind nur bedingt auf bewusste oder unbewusste Fehlbedienung geprüft. Diesem Umstand wollen Entwicklungsstrategien Rechnung tragen, die unter dem Motto „secure by design“ dazu führen, dass die Unterstützung der Sicherheit von Anwendungen von vornherein als eine Aufgabe in den Entwicklungsprozess integriert wird. Was zuerst als zusätzlicher Aufwand erscheinen mag, soll sich am Ende der Entwicklung durch die Einsparung kostenintensiver Tests und Code-Analysen sowie danach notwendiger Programmkorrekturen bezahlt machen. Dabei verbirgt sich hinter dem Begriff „secure by design“, SbD, weniger ein technischer Werkzeugkasten, als vielmehr eine Sammlung von Maßnahmen, die die einzelnen Entwicklungsschritte einer Anwendung begleiten. Die Gesamtheit derartiger Maßnahmen wird daher auch als „Security Development Lifecycle“ (SDL) bezeichnet.

Ein erster Schritt für die inhärente Sicherheit einer Software besteht darin, deren Sicherheit als explizite Anforderung in den Leistungskatalog aufzunehmen. Daraus ergeben sich in den verschiedenen Phasen der Softwareentwicklung automatisch Anknüpfungspunkte für die Überprüfung, wie diese Anforderung jeweils umgesetzt wurde. Dies kann zum Beispiel im Entwurf der Software durch die Verwendung etablierter Entwurfsmuster erfolgen. Derartige Muster können der Software zum einen eine einheitliche Struktur bei vergleichbaren Funktionen geben, was für mehr Transparenz sorgt, zum anderen verringern sie das Risiko, dass bei späteren Änderungen – ggf. durch andere Entwickler – individuelle Programmstrukturen nur unvollständig analysiert und verstanden werden, was wiederum die Programmierung von Seiteneffekten begünstigen würde.

Neben Mustern und Templates gehören Checklisten, Regelungen und sicherheitsrelevante Teststrategien zu einem SbD-Framework. Ergänzt werden diese Maßnahmen durch eine gezielte Schulung der Softwareentwickler für das Thema Sicherheit. Das soll dazu beitragen, dass die entsprechenden Mitarbeiter die Sicherheitsanforderung in ihrem Arbeitsbereich umsetzen und sich nicht allein auf die Lösung fachlicher Probleme und Anforderungen konzentrieren.

Bei der eigentlichen Realisierung der Software gehören Richtlinien des sicheren Programmierens zum Handwerkszeug. Diese umfassen u. a. die Prüfung von Ein- und Ausgaben, Authentifizierung und Zugriffskontrollen, Schutzmaßnahmen für sensible Informationen oder die Umsetzung des Prinzips der geringsten Privilegien, das sicherstellen soll, dass Anwender nicht mehr Berechtigungen haben als unbedingt nötig.

Bei der Umsetzung sicherheitsfördernder Entwicklungsmaßnahmen setzt man durchaus auf Transparenz, in dem Sinne, dass die Sicherheitsmechanismen nicht möglichst geheim gehalten und durch trickreiche Programmierung versteckt werden, sondern dass durch die Offenheit und Verständlichkeit der Implementierung Sicherheitsrisiken besser vermieden bzw. schneller aufgedeckt werden können. Dieser positive Effekt wird höher bewertet als das Risiko, dass offene Softwarekomponenten zusätzliche Informationen für weitere Angriffspunkte liefern.

In Bezug auf die Daten, die in einer Software verarbeitet werden, sieht dies natürlich ganz anders aus – insbesondere dann, wenn es um personenbezogene Daten geht. Und so wurden korrespondierend zu „secure by design“ Entwicklungsstrategien erarbeitet, die den Datenschutz bereits bei der Entwicklung in die Software integrieren sollen. Unter dem Stichwort „privacy by design“ werden hier entsprechende Grundsätze vereint, die den Datenschutz von Anfang an unterstützen sollen und die sich ebenso auf das Thema der allgemeinen Sicherheit übertragen lassen. So lautet – ähnlich wie die Aufnahme von Sicherheit in den Katalog der Anforderungen – einer der Grundsätze, Datenschutz proaktiv und präventiv zu betreiben statt reaktiv und „heilend“. Datenschutz gilt nach einem weiteren Grundsatz als Standard und nicht als die Ausnahme und wird im Softwareentwurf verankert: zunächst gilt alles als geschützt und wird nur bei Bedarf offengelegt. Trotzdem soll Datenschutz nicht im Widerspruch zur vollen Funktionalität der Anwendung stehen bzw. nur auf Kosten von deren möglichem (fachlichen) Nutzen realisierbar sein. Und auch hier soll die Transparenz der Anwendung – nicht die Offenlegung der Daten – für bessere Prüfbarkeit von Systemen und Prozessen sorgen. Durch derlei Maßnahmen lassen sich Sicherheitslücken zwar nie ganz ausschließen, sie leisten aber zumindest einen wesentlichen Beitrag zur jeweils bestmöglichen Sicherheit.

Bewertung

IT-Sicherheit und Datenschutz spielen in der öffentlichen Verwaltung eine besondere Rolle. Daher sollte auch schon bei der Entwicklung von Fachverfahren und anderen Anwendungen auf die Formulierung und Umsetzung von entsprechenden, angemessenen Anforderungen geachtet werden. Sofern Mitarbeiter der öffentlichen Verwaltung unmittelbar in die Entwicklungsprozesse eingebunden sind, sollten

sie für die Themen Softwaresicherheit und Datenschutz sensibilisiert und geschult werden, um die Umsetzung der Anforderungen hinterfragen und ggf. nachvollziehen zu können. Abgestimmte Methodensammlungen erleichtern dabei ggf. die Integration der notwendigen Maßnahmen in den etablierten Software-Lebenszyklus. So widmet z. B. der DIN ISO/IEC-Sicherheitsstandard 27002 der „Beschaffung, Entwicklung und Wartung von Informationssystemen“ ein eigenes Kapitel und schließt dabei insbesondere die „Analyse und Spezifikation von Sicherheitsanforderungen“ mit ein.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Herausgeber
Hessische Zentrale für Datenverarbeitung
Mainzer Straße 29
65185 Wiesbaden
Telefon: 0611 340-0
E-Mail: info@hzd.hessen.de

Verantwortlich
Dr. Markus Beckmann
Telefon: 0611 340-1280
E-Mail: Markus.Beckmann@hzd.hessen.de

Layout
ansicht kommunikationsagentur, www.ansicht.com
Haike Boller (verantwortlich), Anja Wernicke

Grafiken
Titel: fotolia (bubaone)

Druck
Hessisches Landesamt für
Bodenmanagement und Geoinformation
Schaperstraße 16
65195 Wiesbaden

Erscheinungstermin
Januar 2012

HZD
Hessische Zentrale für Datenverarbeitung

Mainzer Straße 29 | 65185 Wiesbaden
Telefon: 06 11 340-0 | Fax: 06 11 340-11 50
E-Mail: info@hzd.hessen.de | www.hzd.hessen.de