HZD
Hessische Zentrale für Datenverarbeitung

HESSEN

TRENDBERICHT **2013**

TRENDBERICHT **2013**

INHALT

VORWORT

Bis vor Kurzem beherrschten zwei technikgetriebene Themen die IT-Fachpresse: die Verlagerung von Anwendungen, Diensten und Ressourcen in „die Cloud" und der Umgang mit privaten Geräten in Firmennetzwerken unter dem Motto „bring your own device". Beide Themen hatten wir im Trendbericht für 2012 vorgestellt und sie sind noch immer in der öffentlichen Wahrnehmung präsent, wenngleich nun verstärkt unter dem Gesichtspunkt, was jenseits aller Begeisterung tatsächlich sinnvoll und sicher machbar ist.

Nun gibt es ein neues Thema, das häufig in den Schlagzeilen auftaucht: Unter dem Stichwort „Big Data" befassen sich die Experten mit der Frage, wie aus vorhandenen Datenbergen neue, relevante Informationen gewonnen werden können. Dahinter verbirgt sich allerdings ein Trend, der sich zum einen schon etwas länger entwickelt und zum anderen mehrere Facetten hat. Das ist zunächst die praktische Handhabung datenintensiver Anwendungen. Klassische Datenbanktechniken reichen oft nicht aus, um neuen Anforderungen gerecht zu werden. Und so entwickeln sich neue Sichtweisen auf ein altes Thema. Desweiteren zwingt die Tatsache, dass Daten bzw. die daraus gewonnenen Informationen einen Wert darstellen können, Unternehmen und Organisationen nicht nur, sie vor Angriffen aus dem „Cyberspace" zu schützen und sich um deren Sicherheit zu kümmern, sondern auch, diese Werte in Governance-Strukturen einzubetten. Dem scheint schließlich ein weiterer Trend entgegenzustehen, der seit kurzer Zeit, dafür aber umso breiter, propagiert wird: Unter dem Stichwort „Open Government" werden die Öffnung von Verwaltungen und Regierungen zu mehr Transparenz gefordert und gefördert – insbesondere durch die kostenlose und öffentliche Bereitstellung ihrer Daten. Diese „Open Data" sollen den Wert der Daten aus öffentlichen Verwaltungen auch für Bürgerinnen und Bürger – und nicht zuletzt Wirtschaftsunternehmen – erschließen. Damit passt auch dieser Trend zu dem neuen Interesse an Daten.

Dass Daten jetzt so stark in den Mittelpunkt des allgemeinen IT-Interesses rücken, mag auf den ersten Blick erstaunen. Schließlich bieten allein Soziale Netzwerke, mobile Endgeräte und Apps permanent Stoff für zahlreiche Artikel. Berücksichtigt man aber, dass die Digital Natives der „Generation Internet" immer mehr in der Arbeitswelt Fuß fassen, ist diese Entwicklung nicht mehr so überraschend. Schließlich sind sie nicht nur mit Computern und deren technischer Vernetzung groß geworden, sondern auch in einer inhaltlich vernetzten Welt. Hier gilt weiterhin: „Content is King" – auch wenn diese Formulierung schon wieder ein paar Jahre alt ist.

Die Themen in diesem Trendbericht spielen – wenngleich mit unterschiedlicher Gewichtung – auch für öffentliche Verwaltungen eine Rolle. Daher haben an diesem Trendbericht wieder viele Experten der HZD mitgewirkt. Der Dank dafür geht insbesondere an Eric Balk, Michael Bopp, Joachim Chilleck, Arno Domack, Thomas Drieß, Stefan Junger, Alberto Kohl, Birgit Lehr, Klaus-Dieter Niebling, Manfred Pospich, Friederike van Roye und Roland Wink.

Wir wünschen Ihnen eine interessante Lektüre und freuen uns über Ihre Kommentare und Einschätzungen.

Markus Beckmann

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 sich ein Trend auf die Verwaltung auswirken kann. Dies kann auf zweierlei Arten erfolgen: Zum einen können Trends zu technischen Änderungen in der IT-Landschaft führen bzw. solche Änderungen ermöglichen. Diese Trends sind daher in dem Maß verwaltungsrelevant, wie sie sich auf einige oder alle IT-Arbeitsplätze im Land auswirken – entweder direkt am Arbeitsplatz oder durch die Gesamtinfrastruktur.

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:

starke
deutliche
mittlere
geringe
keine

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:

sofort
1-2 Jahre
2-4 Jahre
mind. 4 Jahre
noch nicht absehbar

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, dieses in Verwaltung und Unternehmen nutzbar zu machen. Die fünfteilige Skala gibt die Einführungsgeschwindigkeit mit folgenden Werten an:

sofort
1-2 Jahre
2-4 Jahre
mind. 4 Jahre
noch nicht absehbar

01_ ARCHITEKTUREN UND LÖSUNGEN

SICHER UNTERWEGS MIT MOBILE DEVICE MANAGEMENT

Mobile Endgeräte gehören heute zur Standardausstattung einer Unternehmens-IT. Von einzelnen Notebooks, die auf Dienstreisen verwendet werden, bis hin zu einem umfangreichen „Gerätepark", der dazu noch Tablets und Smartphones enthält, ist alles zu finden. Ist die Anbindung und Verwaltung eines Notebooks, das als Standardarbeitsplatz konfiguriert ist, über ein VPN noch relativ einfach, wird die Steuerung und Kontrolle von Endgeräten mit zunehmender Vielfalt der Gerätetypen komplizierter.

Als mit BlackBerrys der Firma RIM eine seinerzeit vergleichsweise komfortable Anbindung an die Firmen-E-Mail über ein Smartphone in die Unternehmen und Verwaltungen drängte, war die Skepsis zunächst groß. Und das nicht nur, weil die Mail über Server der Firma geroutet wurden, sondern auch weil mit den Geräten verschiedene Anwendungen und Nutzungsszenarien in die Unternehmens-IT gelangten, die durch das Gerät – und nicht zentral – gesteuert wurden. Dem Bedürfnis von IT-Verantwortlichen, die Kontrolle über Geräte im eigenen Netz zu bewahren, wurde dadurch Rechnung getragen, dass eine Verwaltungssoftware bereit gestellt wurde, die inzwischen mehr als 500 Sicherheitseinstellungen erlaubt. Damit gilt diese Geräteplattform heute als vorbildlich.

„So viel Aufwand für ein bisschen Mail auf dem Smartphone?" dürfte sich mancher fragen, der lediglich die einfache Bearbeitung von Mails auf Dienstreisen im Fokus hat. Doch die sichere Steuerung von Mobilen Endgeräten – engl. Mobile Device Management (MDM) – ist eine durchaus komplexe Aufgabe, die alle „Lebensphasen" des Gerätes umfassen muss. Zu den Aufgabenfeldern, die ein MDM-System beherrschen bzw. unterstützen muss, zählen:

- **Einrichtung und automatisches Setup der Geräte** – einschließlich Fernkonfiguration oder Bereitstellung bzw. Verteilung von autorisierten Anwendungen, Patch- und Update des Betriebssystems u.v.m.
- **Sicherheitsfunktionen** wie VPN, Verschlüsselung von Daten und deren Übertragung, Fernsperrung oder Fernlöschen von Daten und Anwendungen, Sperrung kompromittierter Systeme
- **Überwachung der Geräte** z. B. Status von Speicher und Netzanbindung, Protokollierung von Systemzugriffen oder Einhaltung von Sicherheitsrichtlinien, Softwarelizenzen, Warnung bei Wechsel der SIM-Karte oder Erkennen von Jailbreaks
- **Support**: Ferndiagnose bei Störungen und Remote-Steuerung des Gerätes durch Administratoren zur Fehlerbehebung

Diese Auswahl von Aufgaben zeigt, dass MDM mehr ist, als die Zuordnung von Geräten, Benutzern und Berechtigungen. Sofern das MDM-System und die zu bedienenden Platt-

formen aufeinander abgestimmt sind, hängt die Komplexität der Aufgabe dann „nur noch" von der Zahl der Nutzer, der Zahl der Geräte und der Zahl der individuellen Anwendungen und Dienste ab. Doch es gibt derzeit allein sieben am Markt etablierte Betriebssysteme für Smartphones und die Innovationszyklen in der IT – insbesondere bei mobilen Geräten – sind sehr kurz. Ständig drängen neue Geräte auf den Markt. Und selbst bei Geräten von einem einzelnen Hersteller kann man nicht sicher sein, dass relativ neue Geräte noch mit der nächsten Generation des Betriebssystems arbeiten können. Wenn man dann noch mobile Geräte verschiedener Hersteller mit unterschiedlichen Leistungsmerkmalen verwalten muss, wird Mobile Device Management schnell zu einer großen Herausforderung. Dabei ist es nicht nur die Art und Weise, in der solche Merkmale – z. B. gerade Sicherheitsfunktionen – konfiguriert und genutzt werden können, sondern ob sie überhaupt vorhanden sind. Hinzu kommt, dass die derzeit verfügbaren MDM-Systeme in der Regel funktionale oder technische Schwerpunkte haben. So warnen entsprechende Presseveröffentlichungen, den Versprechen der Softwarehersteller zu misstrauen, ihre Produkte würden „alle" Aspekte von MDM beherrschen. Zumindest dort, wo höhere Sicherheitsanforderungen bestehen und eine individuelle Betreuung der Endgeräte nicht möglich ist, bedeutet das, dass auf mobilen Geräten nur diejenigen Funktionen unterstützt werden können, die zum einen auf allen technischen Plattformen der Geräte steuerbar sind und die zudem vom MDM-System angemessen unterstützt werden.

Eine weitere Dimension an Komplexität gewinnt das Mobile Device Management, wenn neben Firmengeräten auch noch privat mitbenutzte oder private Geräte im Rahmen einer „Bring your own Device"-Strategie gesteuert werden sollen (s. „BYOD – Bring Your Own Device", HZD-Trendbericht 2012). Selbst wenn dabei nur bestimmte Gerätetypen zugelassen sind, ergeben sich viele zusätzliche Anforderungen an das MDM. In diesem Fall muss zunächst zwischen geschäftlichen bzw. dienstlichen Daten und Anwendungen einerseits und privaten Daten und Anwendungen andererseits unterschieden werden. So muss z. B. geklärt sein, ob private Daten bei einem Verlust des Gerätes per Fernaktivierung ebenfalls gelöscht werden sollen oder nicht. Auch der Zugriff auf private Daten durch Administratoren des Arbeitgebers im Rahmen von Wartungsmaßnahmen muss geregelt oder noch besser gesteuert werden. Schließlich muss auch der Zugriff aus privaten Anwendungen auf dienstliche Daten eingeschränkt werden. Dies ist dann misslich, wenn der Benutzer aber gerade seine gewohnten Werkzeuge auch für dienstliche Arbeiten verwenden möchte, wobei Lizenzfragen einer solchen Mischnutzung hier nicht einmal betrachtet werden sollen. Hier stellt sich zunächst die Frage, ob die Sicherheitsfunktionen, die in den zu betreuenden Betriebssystemen vorhanden sind, ausreichen, um alle Anforderungen an die sichere mobile Nutzung abzudecken. Dieses „native MDM" bietet Lösungen, die für den Anwender leicht handhabbar sind. Allerdings ist man hier von den Funktionen – und auch den Schwachstellen – der eingesetzten Betriebssysteme abhängig.

Die für die Administration einfachste Methode, die private und dienstliche Nutzung eines mobilen Gerätes zu ermöglichen, besteht darin, die Betriebsumgebungen dafür auf dem Gerät zu trennen. So können z. B. alle dienstlichen Anwendungen in einer sog. Sandbox oder einem Container bereitgestellt werden. Zwischen diesen und den übrigen Anwendungen wird Datenaustausch unterbunden. Einige Sandbox-Lösungen bringen eigene Anwendungen mit – insbesondere für das „Personal Information Management" (PIM), also für Kalender-, Mail-, Kontakt- oder Notizfunktionen. Diese Anwendungen unterscheiden sich jedoch in der Regel in Leistungsumfang und Handhabung von den sonst üblichen Anwendungen bzw. mobilen Apps, die für die entsprechenden privaten Aufgaben genutzt werden. Das MDM der BlackBerrys fällt in diese Kategorie.

Eine Variante des Sandbox-Prinzips besteht in einem virtuellen Desktop, mit dem eine normale Arbeitsumgebung auf dem Bildschirm des Geräts abgebildet wird. Deren Nutzbarkeit hängt allerdings davon ab, wie gut sie sich an die mobile Hardware anpasst, denn diese Endgeräte haben oft einen kleineren Bildschirm und ersetzen Maus und Tastatur durch einen Touchscreen.

Neben der umfassenden Sandbox-Methode gibt es auch noch den Ansatz, nur einzelne Anwendungen in Container zu stecken. Bei dieser Methode – auch „Application Wrapping" genannt – kann die Datenübertragung für den Zugriff auf bestimmte Domänen, z. B. Unternehmensdaten, über ein „VPN on demand" abgesichert werden.

Ob die Sandbox- und die Application-Wrapping-Methode langfristig dem Mobile Device Management zugerechnet werden, muss sich zeigen. Da hier der Fokus der Steuerungsaktivitäten mehr auf den Anwendungen als auf dem „Device", also dem Gerät, liegt, wird in diesem Zusammenhang auch von „Mobile Application Management" gesprochen. Schließlich dürften wie der Markt für mobile Endgeräte und Betriebssysteme auch die Methoden und Anwendungen für das Management mobiler Komponenten weiterhin einer ständigen Weiterentwicklung unterliegen.

BEWERTUNG

Das Management mobiler Endgeräte ist in den Verwaltungen geübte Praxis, seit diese Geräte Einzug gehalten haben. Die klassischen Modelle von stark nach außen gesicherten Infrastrukturen und Systemen sind auch beim mobilen Einsatz lange erprobt. Doch die zunehmende Diversifizierung der mobilen Technik erschwert zunehmend deren zentrale Steuerung. Auch die dienstliche und private Mischnutzung stellt das Modell der Absicherung „nach außen" in Frage, denn in diesem Fall verläuft die Grenze zwischen dem Innen der Verwaltungs-IT und dem Außen der privaten Daten und Anwendungen auf dem einzelnen Gerät. Damit hängt die Empfehlung der Experten für einen MDM-Ansatz derzeit noch davon ab, in welchem Maße die Organisation Kontrolle über den Gerätepark an sich hat: Gibt es eine kleine und klar umrissene Palette von Geräten, bietet sich wegen der guten spezifischen Konfigurierbarkeit der Geräte das native MDM an. Mit zunehmender Zahl an Gerätetypen geht die Empfehlung aber stärker in Richtung der Sandbox-Ansätze, da sie eine homogene Sicherheitsarchitektur besser unterstützen. Bis auch native MDM-Systeme einen einheitlichen Sicherheitsansatz angemessen unterstützen, werden Sandbox-Systeme zumindest für umfängliche Nutzung den Vorzug genießen.

Verwaltungsrelevanz: ■■■■

Umsetzungsgeschwindigkeit: ■■■■

Marktreife/Produktverfügbarkeit: ■■■■

DRUCKEN – WO IMMER MAN IST

Im Zusammenhang mit E-Government wird viel an der Beseitigung von Medienbrüchen gearbeitet. Die Vermeidung von Papier und die durchgängig elektronische Abwicklung von Verwaltungsvorgängen soll deren Effizienz verbessern. Auch in anderen Bereichen – sei es in der Privatwirtschaft, in Vereinen und Organisationen oder im privaten Alltag – wird seit Jahren das papierlose Büro propagiert. Doch die Realität sieht anders aus und man kann manchmal den Eindruck gewinnen, dass mit Verbreitung von Büro-IT die Papierberge eher größer als kleiner geworden sind. Das mag häufig stimmen, in anderen Fällen aber auch nicht. Fakt ist aber, dass das Drucken von Daten und Informationen aller Art noch immer hohe Bedeutung im Arbeitsalltag und darüber hinaus hat. Vor diesem Hintergrund stellt die zunehmende Mobilisierung von Arbeit und der Informationstechnik insgesamt eine besondere Herausforderung dar. Oft heißt das, dass Informationen ausschließlich elektronisch im Notebook, Tablet oder Smartphone mit auf Reisen gehen. Selbst wenn die Daten „in der Cloud" oder auf einem normalen Fileserver liegen, steht zunächst einmal nur die virtuelle Variante zur Verfügung. Wenn eventuell doch Papier benötigt werden könnte, bedeutet das allzu oft, dass vorsichtshalber alle in Frage kommenden Informationen ausgedruckt werden, bevor man sich auf den Weg macht. Welche Daten und wie viele Exemplare dann tatsächlich benötigt werden, ist oft schwierig vorab zu klären. Im Zweifelsfall wird dann doch lieber etwas mehr gedruckt ...

Der Wunsch seine Daten „überall" und dann bedarfsgerecht ausdrucken zu können, scheint also nahezuliegen: Es wäre praktisch, wenn man egal mit welchem Gerät man wohin kommt, von dort aus einfach den nächst gelegenen Drucker benutzen könnte. Doch jeder, der auch nur innerhalb des eigenen Büros verschiedene Ausgabegeräte verwenden möchte, weiß, dass das in der Regel nicht so einfach ist: Man muss die Geräte kennen, die richtigen Treiber installiert haben und dann hoffen, dass das ausgesuchte Gerät auch alle benötigten Funktionalitäten – beispielsweise beidseitiges oder farbiges Drucken – beherrscht.

Noch schwieriger wird es, wenn man sich mit seinem mobilen Gerät in fremde IT-Strukturen begibt – zum Beispiel in einer anderen Behörde, bei einem Kunden, bei einer Veranstaltung oder in einem Hotel. Oft kommt man dann um die Mithilfe freundlicher Mitmenschen nicht herum, die die Daten über den eigenen Computer drucken. Doch dieser Weg ist nur für unkritische Daten geeignet. Vertrauliche Daten haben in fremden Händen nichts zu suchen.

Inzwischen gibt es eine ganze Reihe von Lösungen, die das flexible Drucken auf verschiedenen Geräten ermöglichen. Ein erster Schritt sind netzwerkfähige Drucker, die von allen Mitarbeitern genutzt werden können. Dazu müssen sie nicht mehr an einen Arbeitsplatzcomputer angeschlossen werden, der dann auch noch permanent eingeschaltet sein muss. Entsprechende Lösungen sind seit langem etabliert und stehen allen offen, die einen Zugang zum entsprechenden Netzwerk haben. Aber schon externe Gäste scheitern an diesem Ansatz, wenn ihr Gerät nicht für das Netzwerk registriert ist.

Auch für die eigenen Mitarbeiter bringen Netzdrucker manch ein Problem mit sich: So kann der abgestürzte Druckjob eines Kollegen die weitere Nutzung des Druckers beeinträchtigen. Oder in der Eile nimmt jemand anderes die gerade erstellten Ausdrucke irrtümlich mit, was spätestens bei vertraulichen Unterlagen problematisch ist. Eine Lösung für dieses Problem bietet das sogenannte „Pull -" oder „Follow Me-Printing". Dabei wird der Druckauftrag vom eigenen Gerät aus an einen Server geschickt und kann dann von jedem registrierten Drucker aus abgerufen werden. Dazu ist in der Regel eine Authentisierung am Drucker mittels Passwort, ID-Karte oder ähnlicher Funktionen erforderlich. Auch hier muss gewährleistet sein, dass das jeweilige Ausgabegerät alle benötigten Druckfunktionen beherrscht. Fehlende Funktionen muss das Gerät oder die Drucksoftware sinnvoll kompensieren. Für den Ausdruck vertraulicher Informationen ist diese Lösung gut geeignet, denn nur der Besitzer des Dokumentes – oder je nach Lösung auch eine andere, explizit berechtigte Person – kann den Auftrag am Drucker aktivieren. Bei umfangreichen Druckaufträgen hat diese Methode aber den Nachteil, dass die Ausgabe erst startet, wenn der Druck abgerufen wurde. Das kann zu zusätzlichen Wartezeiten oder Fußwegen zum Gerät führen.

Noch flexibler sind Druckanwendungen über das Internet. Mit diesem „Drucken aus der Cloud" soll sich grundsätzlich jeder Drucker auf der Welt nutzen lassen, der über eine Anbindung an das Internet verfügt und für die Benutzung freigegeben ist. Die Anbindung kann bei vielen modernen Geräten direkt per Netzwerkkarte oder über WLAN erfolgen. Ältere Drucker können in der Regel über einen Computer mit dem Internet verbunden werden. Für die Übermittlung der Daten an den Drucker gibt es derzeit zwei Ansätze. Bei dem einen erhält der Drucker eine Mailadresse, an die die zu druckenden Daten geschickt werden können. Bei dem anderen Ansatz vermittelt eine Internetplattform die vom Benutzer hochgeladenen Dokumente an die für ihn registrierten Drucker.

Technisch ist also einiges möglich. Doch echte Anwendungsszenarien sind nur schwer vorstellbar – zumindest dann, wenn sie Geräte einschließen, die so weit vom Nutzer entfernt sind, dass er sich nicht direkt um die Ausgabe oder kleine Störungen – zum Beispiel durch zu wenig Papier – kümmern kann. Auf einem „eigenen", aber weit entfernten Drucker zu drucken, könnte sinnvoll sein, um von unter-

wegs Unterlagen schon einmal bereit zu stellen, die später in Papierform benötigt werden. So könnte zwar der Druck im Home-Office vom Strandcafé aus eventuell Zeit sparen. Das setzt aber voraus, dass die Technik „zuhause" auch absolut zuverlässig arbeitet und über genügend Ressourcen verfügt. Auch für den Druck über „Ländergrenzen" hinweg dürfte in den seltensten Fällen tatsächlichen Bedarf geben. Das Druckergebnis ist in diesem Fall für eine Person am Druckort bestimmt. Da dürfte es in vielen Fällen einfacher sein, die Daten per Mail oder Filesharing-Dienst zu übermitteln und vor Ort auszudrucken. Eine Anwendung könnte jedoch darin bestehen, über weite Entfernungen gedruckte Unikate – eventuell mit eingedrucktem „Wasserzeichen" – zur Verfügung zu stellen, wenn die Weitergabe der Daten gerade nicht gewollt ist.

Nur wenige Nutzer oder Organisationen stellen ihre Druckdienste für Besucher offen zur Verfügung, denn dies würde einen unkontrollierten Zugang zum eigenen Netzwerk bedingen. Dieser wird aber in der Regel nur nach mehr oder weniger aufwändigen Genehmigungsverfahren gewährt – wenn überhaupt. Wenn es hier jedoch gelingt hinreichend sichere und vertrauenswürdige Lösungen zu implementieren, könnte diese Variante des Fremddruckens beispielsweise Außendienstmitarbeitern erlauben, beim Kunden vorhandene Ressourcen zu nutzen.

Sofern es beim „Fremddrucken" um einzelne Seiten geht oder die Ausdrucke beim Eigentümer des Druckers verbleiben, ist der damit verbundene Ressourcenverbrauch unkritisch. Wenn aber viel von fremden Geräten aus gedruckt wird, kann es interessant sein, in die Druckdienste auch eine Ressourcenkontrolle und eine Kostenabrechnung zu integrieren. Solche „Managed Print Services" dienen der Steuerung, Wartung und Überwachung von Druckern und sollen dazu beitragen, den verlässlichen und wirtschaftlichen Betrieb der Geräte zu gewährleisten.

Trotz der interessanten technischen Lösungen stehen Anwender dem mobilen Drucken skeptisch gegenüber. Ein möglicher Grund dafür können Sicherheitsbedenken sein, da die Druckdaten über Infrastrukturen laufen, die nicht der eigenen Kontrolle unterstehen. So gaben in einer Umfrage ein Drittel der Befragten an, mobiles Drucken sei nur ein aktuelles Schlagwort oder ein unbedeutendes Randthema. Auf der anderen Seite ging gut die Hälfte davon aus, dass das Thema in den nächsten Jahren immer wichtiger werde.

BEWERTUNG

Auch wenn die möglichen Anwendungsszenarien noch etwas „gewollt" und konstruiert wirken, würde die Öffnung von Druckressourcen für mobiles Drucken in vielen Fällen die praktische Arbeit erleichtern. Dabei sind aber auf jeden Fall zunächst Sicherheitsfragen zu beantworten. Solange es sich beim mobilen Drucken nicht um ein Massenphänomen handelt, dürfte die Verteilung der Verbrauchskosten oft zweitrangig sein. Investitionen für die Flexibilisierung der eigenen Druckinfrastrukturen dürften da schon eher eine Rolle spielen. Wie auch immer sich der Markt für Unternehmenslösungen oder für Cloudangebote entwickelt, das Thema hat auf jeden Fall einen positiven Nebeneffekt: Beim mobilen Drucken werden Computer und Anwendungen einerseits und Druckerinfrastruktur andererseits entkoppelt. Das setzt voraus, dass Druckdienste stärker standardisiert und flexibler einsetzbar gemacht werden. Im Rahmen eines Output-Managements (s. Artikel <Output-Management>) schließt dies gegebenenfalls auch elektronische Ausgabeformate mit ein. Von dieser Flexibilität könnte jeder Nutzer profitieren – selbst, wenn er in der Regel nur „lokal" druckt.

Verwaltungsrelevanz: ■■■□ – ■■□□

Umsetzungsgeschwindigkeit: ■■■■

Marktreife/Produktverfügbarkeit: ■■■■

RAUS DAMIT! – OUTPUT MANAGEMENT

Verwaltungen, Firmen und Privatpersonen versenden eine Vielzahl von Informationen und Dokumenten. Bei elektronisch erstellten Dokumenten geschieht auch die Zustellung heutzutage zu einem großen Teil auf elektronischem Weg. Doch auch der Versand von Papierdokumenten spielt immer noch eine wichtige Rolle (s. auch S. 9, „Drucken – wo immer man ist"). Bei einzelnen Schriftstücken entscheidet in der Regel der „Produzent" anhand der Art des Dokuments und anhand des Adressaten, ob er es elektronisch versendet oder als „klassische" Papierpost. Beim Massenversand wird die Post entweder über entsprechende Verteiler elektronisch zugestellt oder beim Papierweg über eine Druck- und Kuvertierstraße geleitet.

In den letzten Jahren haben sich neben der einfachen E-Mail eine Reihe weiterer elektronischer Postwege entwickelt. Diese können – wie das elektronische Gerichts- und Verwaltungspostfach (EGVP) – branchenspezifisch sein. Andere Ansätze verknüpften den Mailversand mit Chat- und Kollaborationsfunktionen, konnten sich aber am Markt nicht

durchsetzen. Eine neue Entwicklung stellen sichere Mailverfahren dar, bei denen in Deutschland mit De-Mail ein gesetzlich abgesicherter Standard geschaffen wurde.

Die Nutzung elektronischer Vertriebskanäle bietet neben der hohen Geschwindigkeit der Zustellung in der Regel auch wirtschaftliche Vorteile. Auch nach Umlage der Aufwände für die Bereitstellung der Infrastruktur sind die Kosten für den elektronischen Versand relativ gering. Im privaten Bereich wird E-Mail sogar oft als kostenlos angesehen, weil der dafür notwendige Internetzugang sowieso für andere Angebote genutzt wird und somit vorhanden ist. Bei den stärker abgesicherten elektronischen Verfahren fallen gegebenenfalls auch Stückkosten pro Versandvorgang an. Das beeinflusst zwar bei Privatpersonen die Akzeptanz der Verfahren, erlaubt aber im Hinblick auf die Kostenoptimierung für Unternehmen und Behörden neue Wirtschaftlichkeitsbetrachtungen.

Für große Organisationen bedeutet die breite Palette der möglichen Ausgabekanäle – Einzeldruck, Massendruck, E-Mail, De-Mail oder spezifische Versandarten –, dass zahlreiche Verbindungen zwischen diesen und Anwendungen sowie Verfahren implementiert werden müssen. Eine Optimierung von Kosten anhand der jeweils günstigsten Versandart wird dadurch erschwert. Solange sichergestellt ist, dass der feste Adressatenkreis eines Verfahrens über einen definierten elektronischen Zugang verfügt, kann der gesamte Versand auf diesem Weg erfolgen – sofern das mit Schriftformerfordernissen vereinbar ist. Wenn man aber, wie derzeit noch bei den neuen, verbesserten elektronischen Verfahren damit rechnen muss, dass nur ein Teil der Adressaten diesen Kanal auch nutzt, muss man entweder für alle auf den Papierversand zurückgreifen oder individuell nach Verfügbarkeit den elektronischen Kanal beziehungsweise den Papierversand wählen.

Wenn nahezu jedes Verfahren und jede Anwendung über jeden verfügbaren Postkanal mit jedem Adressaten kommunizieren kann, entsteht ein großes Netz – um nicht zu sagen Gewirr – aus virtuellen Zustellwegen. Daher ist es sinnvoll, die Steuerung des einzelnen Versandstücks über den jeweils besten Weg durch ein sogenanntes Output-Management als zentrale Verteildrehscheibe vorzunehmen. Dies führt zu einer geringeren Zahl von Schnittstellen und reduziert damit die Komplexität der Verbindungsstrukturen. Zudem kann diese Komponente anhand von Informationen über Kosten und Zulässigkeit der verschiedenen Versandarten den optimalen Weg aussuchen. Außerdem können Poststücke aus verschiedenen Anwendungen und Verfahren gebündelt werden, was eventuell zu einer besseren Rabattierung führt.

Insbesondere für Behörden gibt es bei den neuen elektronischen Zustellverfahren noch die Herausforderung der sogenannten Zugangseröffnung. Bevor ein solcher Weg genutzt werden kann, muss der potenzielle Empfänger explizit der Nutzung zugestimmt haben. Dazu reicht die Bekanntgabe der zugehörigen Empfangsadresse in einem Adressverzeichnis nicht aus. Für De-Mail beispielsweise ist dies im De-Mail-Gesetz, §7(3), geregelt. Für ein Output-Management bedeutet das, dass es nicht nur über die entsprechenden Adressen verfügen muss, sondern dass dort auch hinterlegt sein muss, ob beziehungsweise wofür diese genutzt werden dürfen.

Die Aufgaben eines Output-Managements mögen auf den ersten Blick überschaubar erscheinen: Entgegennahme von Dokumenten, Ermittlung von Adressat und Zustellart und Ausgabe auf dem zugehörigen Kanal. Durch die Vielzahl der möglichen Verbindungen und der benötigten Detailinformationen kann eine solche Komponente aber durchaus als komplex angesehen werden. Zudem muss bei den elektronischen Kanälen in der Regel auch der Posteingang implementiert werden. Trotzdem stellt eine zentrale Lösung gegenüber den vielen Einzelverbindungen und im Hinblick auf eine Kostenoptimierung beim Versand eine Verbesserung dar.

BEWERTUNG

Gerade große Verwaltungen nutzen eine Vielzahl von Zustellarten für ihre elektronisch erzeugten Dokumente. Im Hinblick auf die durchgängig elektronische Durchführung von Verfahren und dazu die Vermeidung von Medienbrüchen ist eine optimale Nutzung der elektronischen Kanäle erstrebenswert. Auch unter Kostenaspekten besitzt Output-Management im öffentlichen Bereich ein Optimierungspotenzial – gerade für die papiergebundene Zustellung. Die schrittweise Anbindung einzelner Anwendungen und Verfahren an das Output-Management kann relativ zügig erfolgen. Die Umstellung einer vollständigen Verwaltungslandschaft – bis hin zu normalen Office-Anwendungen an den Arbeitsplätzen – ist aber eher ein mittel- bis langfristig angelegtes Unterfangen.

Verwaltungsrelevanz: ■■■■

Umsetzungsgeschwindigkeit: ■■■■ – ■■□□

Marktreife/Produktverfügbarkeit: ■■■■

02_ DATEN, INFORMATION UND WISSEN

BIG DATA

Ein Trend ist die Entwicklung eines Sachverhalts über eine gewisse Zeit und dient oft der Vorhersage der künftigen Veränderungen. Ein Hype dagegen ist so etwas wie eine Modeerscheinung. In der IT erkennt man einen Hype oft daran, dass alle darüber reden und plötzlich schon seit Jahren Erfahrung damit haben – selbst wenn das Thema noch neu ist.

Eins der aktuellen Hype-Themen ist derzeit „Big Data". Was es damit auf sich hat und welche Trends sich dahinter verbergen, soll in diesem Trend-Spezial betrachtet werden.

GRÖSSE ALLEIN GENÜGT NICHT ...

„Big Data" heißt einfach übersetzt „große Daten" – oder besser: „große Datenmengen". Unabhängig davon, ob man unter diesem Schlagwort Werkzeuge, Technologien, Methoden oder aber die Daten an sich versteht – es geht bei dem Thema auf jeden Fall um große Mengen von Daten und deren Verarbeitung. Doch dies wirft schon die Frage auf, was denn überhaupt „groß" im Zusammenhang mit Datenmengen bedeutet. Wer die Entwicklung von der seinerzeit „großen" 3,5"-Diskette mit 1,44 MB Speicherkapazität über die sagenhafte 40 MB-Festplatte in den ersten PCs zu CD-ROMs (750 MB) bis hin zu Terabyte-großen Solid State Drives (SSDs) erlebt hat, weiß auch, dass jedes Speichermedium, das auf den ersten Blick groß erscheint, früher oder später voll ist. Es ist daher schwierig, eine Definition für „große Datenmenge" zu finden, die universell ist und längere Zeit bestand hat.

Der Trend zu immer weiter wachsenden Datenbergen hat mehrere Ursachen: Das Volumen der Daten wird zum einen durch deren Beschaffenheit bestimmt. Ähnlich wie sich die Speicherkapazität von Datenträgern entwickelt hat, hat sich auch die Art der Daten weiterentwickelt. Nach zunächst einfachen, dann formatierten Texten und später Bildern zählen heute Ton- und Videodaten zu den Standardformaten, die sowohl im privaten als auch professionellen Umfeld genutzt und dazu gespeichert werden. Auch die Anzahl der Datensätze und die Zahl der Quellen, die Daten generieren, steigen weiter an und schließlich wollen immer mehr

TREND SPEZIAL

Nutzer von den Daten Gebrauch machen. So enthielt ein Soziales Netzwerk Anfang des Jahres 2012 ca. 40 Milliarden Fotos und bei einem Video-Portal wurden pro Minute etwa 35 Stunden an Filmmaterial hochgeladen. Sensoren und Kontrollsysteme aller Art liefern permanente Ströme von Zustandsdaten. Und mit der Verbreitung von E-Business und E-Government werden auch in der Privatwirtschaft und in der öffentlichen Verwaltung die Datenbestände immer größer.

Die Datenmenge ist beim Thema Big Data zwar wichtig, sie allein macht das Thema aber noch nicht aus – und so gibt es auch für das Datenvolumen keinen Schwellwert, ab dem man von „big" spricht.

... AUCH STRUKTUR ...

Ein weiterer Faktor, der bei Big Data eine Rolle spielt, ist die Struktur der Daten. Unter der Struktur von Daten versteht man das Muster ihrer einzelnen Datenelemente und deren Beziehungen: Aus den Datenelementen Straße, Hausnummer, Postleitzahl und Ort lassen sich z. B. Adressdaten konstruieren. Diese können mit Personendaten wie Name, Vorname, Geburtsdatum und Geschlecht zu Personal- oder Kundendaten kombiniert werden. Solche gut strukturierten Daten lassen sich vergleichsweise leicht automatisch verarbeiten – auch in großen Mengen. Fortlaufende Texte sind dagegen nur wenig strukturiert. Sie haben evtl. einen Titel, eine Einleitung und einzelne Kapitel mit Überschriften, aber ansonsten nur wenig Struktur. Eine Frage wie: „In welchen Trendartikeln in diesem Heft geht es um Daten?" erfordert schon etwas mehr Analyseaufwand als die einfache Adresssuche in einer Tabelle. Beschränkt man die Suche nach Artikeln über Daten dann nicht auf diesen Trendbericht, sondern dehnt sie auf Beiträge aus verschiedenen Quellen – z. B. Blogs – mit unterschiedlichen Textstrukturen aus, wird daraus schnell eine Fleißarbeit. Noch weniger Struktur weisen Bild- und Videodaten auf. Auch wenn diese mit Titeln und Schlagworten versehen werden, haben die eigentlichen Bilddaten nur wenig Struktur. Die technische Struktur – etwa die Bildpunkte – ist dabei in der Regel von geringer Bedeutung, denn wer würde z. B. seine Urlaubsbilder schon nach der Farbe des ersten Pixels sortieren. Um semantische Informationen zu ihren Inhalten zu erhalten, muss man die Bilder aufwändig analysieren. Hierfür wie auch für Textanalysen und viele andere Fragestellungen im Zusammenhang mit Datenstrukturen gibt es Spezialwerkzeuge, die auf die jeweils anstehende Aufgabe zugeschnitten sind.

Die Verschiedenartigkeit der Datenstrukturen und die Vielzahl von unterschiedlichen Datenquellen geben einen Hinweis auf ein weiteres Merkmal von Big Data – nämlich die Komplexität der Datensammlungen. Eine der großen Herausforderungen, wenn es darum geht, Nutzen aus vorhandenen Daten zu ziehen, besteht darin, Daten aus verschiedenen Quellen mit unterschiedlichen Strukturen und Datenformaten miteinander in Beziehung zu setzen. Die oft schlechten Suchergebnisse von Internetportalen, die auf Personensuchen spezialisiert sind und dazu verschie-

denste Quellen anzapfen, vermitteln einen Eindruck von der Schwierigkeit, die richtigen Daten zusammenzuführen. Selbst für gut strukturierte Daten in Verwaltungsanwendungen ist diese Zusammenführung – abgesehen von häufig auftretenden Datenschutzaspekten – eine Herausforderung und hat zu zahlreichen Standardisierungsvorhaben geführt (z. B. sog. X-ÖV-Standards).

... UND GESCHWINDIGKEIT

Als steckten in den genannten Aspekten von Big Data nicht schon genug Herausforderungen, kommt eine weitere hinzu: Geschwindigkeit. Es gibt immer mehr Bereiche, in denen die Verarbeitung großer Datenmengen schnell gehen muss. Klassische Anwendungen zur Verarbeitung von Geschäftsdaten für die sog. Business Intelligence (BI) beherrschen zwar ggf. die Konsolidierung und Integration von Daten, deren Speicherung in einem sog. Data Warehouse sowie vielfältige Analysen, die Verarbeitungsschritte sind jedoch oft langwierig, so dass an manchen Stellen in diesem Zusammenhang von der Verarbeitung „historischer Daten" gesprochen wird. Für interne Geschäftsberichte, die z. B. quartalsweise erstellt werden, ist es zwar sinnvoll, wenn der Berichtszeitraum abgeschlossen ist, bevor Daten analysiert werden, und es kommt hier in der Regel auf ein paar Stunden oder Tage an Bearbeitungszeit nicht an. Viele andere Aufgaben, die die Verarbeitung großer Datenmengen einschließen, sind aber zeitkritisch und müssen ggf. in „Echtzeit" erledigt werden. So hat sich als ein Anwendungsgebiet für Big Data die Zustandsanalyse komplexer Systeme herauskristallisiert. In Rechenzentren oder IT-Infrastrukturen, im Verkehr, im Gesundheitswesen, bei der Produktionssteuerung, in der Logistik und vielen anderen Bereichen fallen viele Daten an. Diese oft kontinuierlichen Datenströme aus Sensoren, Logfiles und auch manuellen Eingaben müssen zeitnah verarbeitet werden, um z. B. Störungen schnell zu erkennen oder – noch besser – bevorstehende Ereignisse vorhersagen zu können. Das Herausfiltern von Symptomen oder Warnhinweisen ist für jede einzelne Datenquelle evtl. ein sehr einfacher und schnell zu erledigender Vorgang. Durch die Menge von Daten pro Messstelle und über viele Stellen hinweg wird die zeitnahe Verarbeitung zu einer Gesamtsicht zu einer Herausforderung.

In Bereichen, in denen Zeit ein nicht so kritischer Faktor ist, spielen Big Data-Ansätze eine andere Stärke aus: die Verarbeitung unterschiedlichster, auch unstrukturierter Daten aus vielen Quellen. So kann z. B. ein Unternehmen Informationen über seine Kunden aus der Presse, von Internetseiten, aus Kundeninformationssystemen mit den klassischen Kundendaten aus Buchführung oder Vertragsmanagement zusammenführen, um die Entwicklung der Kundenbeziehung zu analysieren. Bei den zuerst genannten Informationen handelt es sich zumeist um nicht oder nur wenig strukturierte Daten. Hier geht es nicht allein darum, den Namen des Kunden in einem Artikel zu finden, sondern auch den Zusammenhang zu analysieren, in dem der Name auftaucht.

MAPREDUCE

All die genannten Teilaufgaben – Filtern von Sensordaten, Erkennen von kritischen Messwerten, Analysieren von Texten oder Bildern usw. – werden von Big Data-Anwendungen nicht automatisch erledigt oder als universeller Dienst mitgeliefert. Die Anbindung konkreter Systeme und die Analyse spezifischer Fragestellungen müssen in der Regel vor Ort entwickelt und ggf. pro Datenquelle implementiert werden. Die Stärke von Big Data-Anwendungen besteht darin, die „Intelligenz" und die dafür benötigte Rechenleistung geschickt zu verteilen und die Zusammenführung und Konsolidierung der Teilergebnisse zu vereinfachen.

Ein wesentliches Instrument bei der Realisierung von Big Data-Anwendungen ist der sog. „MapReduce"-Algorithmus. Das Prinzip dieses Algorithmus ähnelt dem von „Teilen und Herrschen" – also dem Zerlegen einer großen Aufgabe in kleine Teilaufgaben, die sich lösen lassen. Bei klassischen Datenbanksystemen ist dagegen auch die Verarbeitung prinzipiell parallelisierbarer Aufgaben wie Abfragen letztlich auf einen Prozessorkern beschränkt. Diese Beschränkung wird mittels MapReduce aufgelöst und eine einzelne Abfrage kann von mehreren Prozessorkernen parallel verarbeitet werden.

Bei der Anwendung von MapReduce wird die Verarbeitung eines großen Datenbestandes aufgeteilt. Technisch implementiert wird das MapReduce Verarbeitungsmodell durch Programm-Frameworks wie Hadoop. Wenn die Leistung der aktuell vorhandenen Knoten des Computer-Clusters nicht ausreichen sollte, um die Verarbeitung in der gewünschten Zeit zu erledigen, dann erlauben es diese Frameworks, Rechner-Knoten (bei Hadoop „Data Nodes") hinzuzufügen, ohne dabei das Verarbeitungsprinzip zu verändern. Der Lösungsansatz heißt dabei immer „Add more nodes".

Bei vielen Big Data-Anwendungen können die Datenbestände auch von vorne herein aufgeteilt sein wie etwa in den oben genannten Beispielen der Analyse von Sensor- oder Log-Daten. In der ersten Phase von MapReduce werden die Daten der kleinen Datenbestände entsprechend der anstehenden Aufgabe bearbeitet und auf ein Teilergebnis abgebildet (engl. „map"). Die kann z. B. das Zählen von Worten in einem Text sein, das Auffinden von Störungsmeldungen oder – etwas komplexer – die inhaltliche Analyse einzelner Bilder aus einem Video. Selbst wenn die Eingangsdaten sehr unterschiedlicher Art sein können, müssen die Ergebnisse der einzelnen Analysen gleichartig sein, denn in der

zweiten Phase – der Reduktion (engl. Reduce) – werden diese Teilergebnisse zu einem Gesamtergebnis zusammengeführt. Auch hier kann die Arbeit ggf. parallelisiert werden. So können beim Zählen von Wörtern in verschiedenen Texten die Teilergebnisse für ein Wort auf einem Rechner addiert werden, während gleichzeitig ein anderer Rechner die Häufigkeiten eines anderen Wortes berechnet usw. Eine der bekanntesten Anwendungen von MapReduce ist der Aufbau des Suchindex bei der Internetsuche der Firma Google, die auch ein Patent auf den Programmframework hat.

Wie bei jedem Hype-Thema, das von den Anbietern einschlägiger Lösungen vollmundig beworben wird, wurden inzwischen auch zu Big Data kritische Stimmen laut.

Zum einen stehen dabei die Aufwände im Fokus, die zu leisten sind, bevor Nutzen aus den neuen Analysen gezogen werden kann. Neben Kosten für neue Komponenten – z. B. für auf die verteilte Arbeit spezialisierte Rechner, sog. Appliances, – sind dies auch Aufwände für die Bereitstellung von Know-how zur Entwicklung und Implementierung der neuen Analyseverfahren. Auch die Qualität der Ausgangsdaten spielt eine wichtige Rolle. So können schon einfache Aufgaben wie das Zählen von Wörtern auf der semantischen Ebene durch den Gebrauch von Synonymen und Homonymen (sog. „Teekesselchen") schnell erschwert werden. Daher ist es nicht verwunderlich, dass im Umfeld von Big Data-Projekten Data Governance zum Trendthema wird (s. S. 16, „Data Governance").

Auch die Komplexität einer Big Data-Analyse kann ein kritischer Faktor sein. Um ein vollständiges Bild einer komplexen Umgebung zu erhalten, müssen alle Daten erhoben und in die Analyse einbezogen werden. Dies kann sehr viele Messstellen bzw. die Anbindung vieler verschiedener Systeme erfordern. Auch die Implementierung der Teilanalysen und der geordneten Zusammenführung der Teilergebnisse – z. B. die einzelnen Map- resp. Reduce-Funktionen bei MapReduce – können erheblichen Aufwand erzeugen und zu komplexen Softwarearchitekturen führen.

Schließlich sind auch Datensicherheit und Datenschutz Themen, mit denen sich Big Data-Vorhaben befassen müssen. Das Sammeln und Verarbeiten großer Datenmengen bringt dazu eine Reihe von Herausforderungen mit. Es stellt sich z. B. die Frage, wer in welchem Verarbeitungsschritt welche Daten – geschweige denn „alles" – sehen darf. So wurde in einer Umfrage zur Befassung von Unternehmen mit Big Data das Thema Datensicherheit vielfach als entscheidend dafür genannt, zunächst keine entsprechenden Projekte aufzusetzen.

BEWERTUNG

„Big Data" bezeichnet Methoden und Techniken, die neue Erkenntnisse aus bisher wenig oder gar nicht genutzten Daten versprechen. Solche Daten gibt es auch in Verwaltungen. Nicht nur im technischen Bereich, sondern auch in Fachanwendungen könnten neue, verbesserte Analysetechniken neue Zusammenhänge sichtbar machen. So herrscht derzeit großes Interesse an Analysen von Freitextfeldern in Formularen und deren Verknüpfung mit strukturierten Daten der Fachanwendungen. Entsprechend der schematischen Formel „Information = Daten + Kontext" können die stark verteilt ableitenden Big Data-Strategien viele Daten in neue Zusammenhänge bringen und somit neue Informationen erzeugen. Big Data ist mehr als das Sammeln und Anhäufen von großen Datenbergen. Bevor man sich auf die neuen und interessanten Techniken und Methoden stürzt, sollte man daher zunächst klären, welche konkrete neue Fragestellung mit einer Big Data-Lösung beantwortet werden soll. Zudem muss bedacht werden, dass Big Data-Produkte nicht aus sich heraus wundersame Erkenntnisse generieren können. Sie bieten in der Regel das Werkzeug, um den technischen Rahmen einer Analyselösung zu bauen. Die Analyse der Daten muss in der Regel in einem Projekt mit dem Fachwissen der Anwender realisiert werden.

Verwaltungsrelevanz: ■■■□

Umsetzungsgeschwindigkeit: ■■■□ – ■■□□

Marktreife/Produktverfügbarkeit: ■■■■ – ■■■□

DATA GOVERNANCE

Daten sind „Darstellungen" von Informationen – und da es hier um IT-Trends geht, stehen „maschinenlesbare" Darstellungen im Vordergrund. Im Folgenden werden die Begriffe „Daten" und „Information" in diesem Sinne synonym verwendet. Dies sei vorausgeschickt, da neben dem Begriff „Data Governance" oft auch die Bezeichnung „Information Governance" für das gleiche Thema verwendet wird.

Jeder, der schon einmal das Verzeichnis der Telefonnummern von Freunden und Bekannten auf seinem Handy versehentlich gelöscht hat, weiß, dass Daten einen gewissen Wert darstellen. Die Telefonnummern nicht zu haben, kann z. B. dazu führen, dass man Freunde nicht treffen kann, und sie wieder in das Handy einzutippen, „kostet" wertvolle Zeit. Diese mag kürzer sein, wenn man ein Backup der Daten hat, das man wieder einspielen kann, – lästig ist so ein Datenverlust auch in diesem Fall.

Unternehmen und Verwaltungen verfügen über große Mengen von Daten. Diese liegen teilweise strukturiert vor, d. h. – vereinfacht gesagt – in Formular- oder Tabellenform. Der größte Teil ist aber nur wenig strukturiert oder ganz unstrukturiert und findet sich z. B. in Verträgen, Briefen und E-Mails, Konzepten, Stellungnahmen, Rechnungen usw. Wenn schon das Vorhandensein oder Fehlen von Telefonnummern spürbare Auswirkungen haben kann, wird schnell klar, dass die Gesamtheit der Daten eines Unternehmens oder einer Verwaltung für diese Organisation immense Bedeutung hat. Dieser Bedeutung wird in der Regel durch Mechanismen der Datensicherung, der IT-Sicherheit und des Datenschutzes Rechnung getragen. Der unternehmerische Wert der Daten wird dabei aber nicht betrachtet – zumindest solange sie nicht explizit irgendwo eingekauft werden.

Data Governance berücksichtigt diesen weitergehenden Wert von Daten und betrachtet sie unter dem Slogan „Information as an Asset" als Anlagengüter. Das bedeutet zwar nicht, dass jede Telefonnummer als eigenständiger Wert in der Buchhaltung auftaucht, vielmehr werden für den Umgang mit Daten Anforderungen definiert und daraus Aufgaben abgeleitet.

Die Anforderungen betreffen klassische Themen wie Sicherheit und Datenschutz (s. o.), aber auch

- Datenqualität,
- Beitrag zur Prozessqualität,
- Erfüllung von Compliance-Anforderungen oder
- Vertrauenswürdigkeit von Daten.

Die Datenqualität muss sowohl auf syntaktischer und auf semantischer Ebene gewährleistet sein. D. h. Daten müssen korrekt „geschrieben" sein und sie müssen die richtigen Dinge bezeichnen (z. B. „M. Mustermann" = „Mustermann, Max"?). Durch korrekte und aktuelle Daten sollen Prozesse besser gesteuert werden. So kann durch das Löschen – bzw. das Markieren als „nicht aktuell" – nicht mehr gültiger Daten vermieden werden, dass ein Prozess ins Leere läuft. In strukturierten Verfahren sollte das der Normalfall sein. Aber oft erhält man z. B. Firmenpost, die an ehemalige Kollegen adressiert ist.

Schnell und verlässlich Auskunft über Geschäftsabläufe geben zu können, ist heutzutage für Unternehmen wie auch Verwaltungen eine wichtige Anforderung. Diese wird zum Teil durch Vorschriften oder Gesetze erhoben und setzt vertrauenswürdige Daten voraus. Aber auch im Umgang mit anderen Organisationen sind vertrauenswürdige Daten wichtig (z. B. nachvollziehbare Projektreferenzen).

Data Governance ist also ein Regelungs- und Steuerungssystem, das einer Organisation helfen soll, die Anforderungen an seine Daten zu erfüllen. Dementsprechend werden im Rahmen der Data Governance die Prozesse, Rollen und Regeln – und schließlich auch die technischen Hilfsmittel – festgelegt, durch die der Wert ihrer Daten für die Organisation erschlossen wird.

So muss etwa geregelt werden, wer welche Daten lesen darf bzw. muss, um seinen Berichtspflichten nachkommen zu können. Die Prozesse können z. B. der Prüfung von Daten schon bei deren Erfassung dienen und sie begleiten die Daten während ihres weiteren Lebenszyklus. Dabei ist es wichtig, Daten nicht nur isoliert in ihrem jeweiligen Anwendungszusammenhang zu betrachten. Qualität und Verlässlichkeit der Daten über verschiedene Anwendungen sicherzustellen ist für das Gesamtunternehmen sehr wichtig. Daher sollten Werkzeuge zur Unterstützung der Data Governance-Prozesse serviceorientiert gestaltet werden, um sie möglichst flexibel in verschiedenen Anwendungen nutzen zu können. Durch geeignete Prozesse wird Data Governance effektiv, durch passende und nicht zu schwerfällige IT-Werkzeuge wird sie effizient.

Eine wichtige anwendungsübergreifende Komponente für ein Data Governance-System ist ein Verzeichnis, in dem die vorhandenen Typen von Daten, deren Ursprung und Verwendung sowie Beziehungen untereinander beschrieben sind. Strukturierte Daten lassen sich hier vergleichsweise einfach – evtl. sogar automatisch erfassen. Für wenig bzw. unstrukturierte Daten (z. B. „fachliche Ansprechpartner" in Verträgen) ist dies in der Regel aufwändig – aber genauso notwendig. Auch die Erklärung der fachlichen Bedeutung der Daten in einem Glossar ist für eine unternehmensweit einheitliche Sicht auf die vorhandenen Informationen wichtig.

Modelle zur Data Governance sind oft sehr umfangreich und scheinen aufwändig zu implementieren. Doch wie bei allen komplexen Aufgaben ist es wichtig, in angemessenem Rahmen mit deren Erledigung zu beginnen. So wird es als ein wesentlicher Erfolgsfaktor für Data Governance-Programme angesehen, zunächst ein konkretes Geschäftsproblem zu identifizieren, das durch die zu entwickelnden Prozesse, Regeln und Rollen gelöst werden soll. Dadurch kann deutlich werden, dass der Aufwand für Datenqualität usw. nicht Selbstzweck ist, sondern bei der Bewältigung tatsächlich vorhandener Herausforderungen hilft.

Ein weiterer Erfolgsfaktor besteht in der Unterstützung durch das Management. Die Leitung von Behörden muss die Bedeutung der Data Governance für die Organisation vermitteln, um die notwendigen aber manchmal komplizierten und aufwändigen Maßnahmen – insbesondere der Einführung – umsetzen zu können.

Der wichtigste Erfolgsfaktor für Data Governance sind schließlich die Mitarbeiter, die die Maßnahmen in ihrer täglichen Arbeit umsetzen müssen. Die Erfassung von Metadaten, die Prüfung erfasster Daten, der Abgleich vorhandener Daten u. v. m. sind nur dann erfolgreich umsetzbar, wenn die Bedeutung „guter" Daten für die Lösung echter Probleme vermittelt wird. In manchen Organisationen kümmern sich eigens eingerichtete sog. „Data Stewards" um die operative Data Governance und sorgen dafür, dass z. B. vorhandene Daten wieder verwendet werden.

Dass Data Governance gerade jetzt an Popularität und Bedeutung gewinnt, ist nicht verwunderlich, auch wenn das Thema bereits einige Jahre alt ist: Die Menge der verfügbaren – insbesondere unstrukturierten – Daten steigt weiterhin rasant an. Auch der Trend zu heterogenen und verteilten IT-Systemen steigert die Komplexität der Datenverarbeitung und führt evtl. sogar zu zusätzlichen Problemen. Umso wichtiger werden die oben angesprochenen serviceorientierten Werkzeuge zur Unterstützung der Data Governance-Prozesse. Durch Trends wie mobile IT und „always on" steigt der Druck, Daten zur Lösung von Problemen schnell verfügbar zu haben. Und schließlich wächst auf die Zahl der Nutzer von IT – und damit auch der vorhandenen Daten – kontinuierlich an.

BEWERTUNG

Viele Daten mögen für Verwaltungen nicht in dem Sinne „unternehmenskritisch" sein, wie sie das für privatwirtschaftliche Unternehmen sind. Gerade das im Zusammenhang mit Data Governance oft genannte Feld der Kundendaten, spielt hier eine wesentlich geringere Rolle, da Verwaltungsprodukte bisher in der Regel nicht auf einem „Markt" bestehen müssen. Daher ist es hier besonders wichtig, zunächst ein durch Data Governance zu lösendes Problem zu identifizieren, bevor Maßnahmen ergriffen werden. So wächst in öffentlichen Einrichtungen z. B. auch die Notwendigkeit, schnell auskunftsfähig zu sein. Wenn etwa die Frage nach Effektivität und Effizienz von Verwaltung gestellt wird, werden schnelle und vertrauenswürdige Informationen erwartet. Die fachlich getriebene Verbesserung der Handhabung ihrer Daten gewinnt also auch für öffentliche Verwaltungen an Bedeutung.

Verwaltungsrelevanz: ■■■■

Umsetzungsgeschwindigkeit: ■■■□ – ■■□□

Marktreife/Produktverfügbarkeit: ■■■■

WAS MAN (NICHT) IM KOPF HAT ... IN-MEMORY-DATENBANKEN

Wer die Fachpresse zum Thema In-Memory-Datenbanken verfolgt, konnte zeitweise den Eindruck gewinnen, dass sich hinter diesem Schlagwort lediglich der Produktwettstreit zweier großer Software- bzw. Datenbankhersteller verbirgt. Doch das Thema ist weiter gefasst, technisch vielfältiger und verdient daher eine genauere Betrachtung.

Die Aufbewahrung von Daten ist neben deren Verarbeitung eines der großen Themen in der Informationstechnik. Nicht erst seit dem Aufkommen der Computer werden große Datenbestände zentral vorgehalten, um für den Wissensgewinn schnell verfügbar zu sein. Schon in der Antike war die berühmte Bibliothek von Alexandria an eine Forschungseinrichtung angegliedert. Im Zeitalter der elektronischen Rechner und Speicher ist die Recherche nach Informationen in der Regel nicht mehr ganz so aufregend wie die Suche nach einem verschollenen Buch in dem Roman „Der Name der Rose". Doch angesichts immer größer werdender Datenmengen dauert auch heute noch die Analyse mancher Fragestellungen mehrere Tage. Die Erhöhung der Rechenleistung und die Beschleunigung von Speichermedien haben dazu beigetragen, dass heute Informationen aus Datenbeständen gewonnen werden können, die noch vor wenigen Jahren erst vorgelegen hätten, wenn sie bereits veraltet und damit uninteressant gewesen wären.

Der Bedarf an schneller Informationsgewinnung wird immer größer. Und so gibt es verschiedene Ansätze, die nicht allein auf immer schnellere Geräte vertrösten, sondern an der Systemarchitektur ansetzen, um die Datenverarbeitung zu beschleunigen. Neben der Parallelisierung in Big-Data-Anwendungen stellen sog. In-Memory-Datenbanken, bei denen komplette Datenbanken im Hauptspeicher gehalten werden, einen solchen Ansatz dar.

Die Stärke von In-Memory-Datenbanken resultiert aus einer aufeinander abgestimmten Hard- und Software-Architektur, die für die schnelle Verarbeitung von Daten optimiert ist. Ähnlich wie bei dem Bild der Bibliothek neben der Forschungsanstalt, zwischen denen Bücher hin und her getragen werden, gibt es auch in Computern Komponenten für die Datenhaltung und für die eigentliche Verarbeitung. Auch zwischen diesen Komponenten müssen die Daten, die verarbeitet werden sollen, transportiert werden. Schon bei der Büroarbeit merkt man oft einen deutlichen Unterschied in der Geschwindigkeit zwischen Aktionen, die mit im Speicher befindlichen Daten ablaufen, und solchen, die Daten von der Festplatte oder aus dem Netz benötigen. Wenn nun Operationen auf großen Datenbeständen in einer Datenbank durchgeführt werden, können sich viele, eigentlich kurze, Transportzeiten zu langen Verarbeitungszeiten addieren. Eine naheliegende Strategie zur Optimierung von Zugriffszeiten besteht darin, Daten, die häufig verwendet werden, in einem schnellen Pufferspeicher – einem sog. Cache – abzulegen. Solche Zwischenspeicher werden z. B. in Web-Browsern und Web-Servern verwendet, um häufig besuchte Seiten schneller ausliefern zu können. In Festplatten und anderen Speichern wird ein Cache verwendet, um die Transportgeschwindigkeit zu erhöhen und Schwankungen in den Zugriffszeiten auszugleichen. Auch im eigentlichen Rechner werden Daten zwischengespeichert. Dabei werden oft mehrstufige Speicher aufgebaut, die sich in Größe und Zugriffsgeschwindigkeit noch einmal unterscheiden. Dabei gilt: Je näher am Rechenkern der Speicher liegt, desto schneller kann der Zugriff erfolgen.

Schnelle Speicherstrukturen bilden den technischen Kern von In-Memory-Datenbanken, denn „in memory" heißt zunächst nichts anderes als „im Gedächtnis" – oder technisch gesprochen: „im Speicher". Bei den aktuell verbreiteten Datenbanksystemen ist der Hauptspeicher wesentlich kleiner als die Datenbank und es können immer nur Teile der Datenbank im Hauptspeicher gehalten werden. Ziel ist es dabei, immer die Daten in einem gemeinsamen Cache im Hauptspeicher zu halten, auf die am häufigsten zugegriffen wird, und seltener benötigte Daten wieder auszulagern. Im Hauptspeicher Cache sind aber immer nur Teile von Datenbankobjekten oder allenfalls komplette Tabellen. Wenn die Trefferrate auf diesen Cache hoch ist, sind die Datenbank-Zugriffe performant und erzeugen keine den Arbeitsfluss störenden Wartezeiten. Sind die benötigten Daten dagegen nicht im Cache vorhanden, müssen sie erst mit langsamen Festplattenzugriffen in den Hauptspeicher geladen werden. Die resultierenden Verzögerungen können sich zu störenden Wartezeiten summieren. Diese Probleme haben In-Memory-Datenbanken konzeptionell nicht, weil immer die komplette Datenbank im Hauptspeicher verfügbar ist.

Bei diesen Datenbanksystemen werden alle Daten im Hauptspeicher gehalten. Bei Speichergrößen von bis zu zwei Terabyte steht dabei heute erheblich mehr Platz für Daten zu Verfügung, als noch vor wenigen Jahren auf Consumer-Festplatten. Eine weitere technische Komponente zur Optimierung der Hardware stellen CPUs mit mehreren Rechenkernen dar. Dadurch kann die Verarbeitung in einem einzelnen Rechner parallelisiert werden. Spezielle Maschinen für In-Memory-Verarbeitung sind mit bis zu 40 CPU-Kernen ausgestattet. Die resultierende Prozessorleistung können sie auch besser nutzen, weil Prozessoren nicht oder nur selten durch Wartezeiten auf Datenbankzugriffe blockiert sind.

Die Optimierung der Systemarchitektur im Hinblick auf die Verarbeitungsgeschwindigkeit wirkt sich auch auf die Software aus. Klassische, relationale Datenbanken verarbeiten Daten in Transaktionen, die in der Regel auf einzelnen fachlichen Datenobjekten ausgeführt werden. Das bedeutet, dass die einzelnen Datenobjekte aus dem Speicher geholt, verarbeitet und wieder zurückgeschrieben werden müssen. Wenn nur einzelne Datenfelder bei einer Operation von Interesse sind, kann das zu viel Overhead beim Transport der Daten führen. Zur Verbesserung der Geschwindigkeit arbeiten daher In-Memory-Datenbanken oft spaltenorientiert (vgl. S. 20, „Nicht nur, aber auch? –NoSQL"). Das bedeutet, dass die Operationen jeweils nur auf den betroffenen Datenfeldern – sprich in einer Spalte der Datentabelle – ausgeführt werden. Will man beispielsweise in einer klassischen Datenbank, in der Umsatzinformationen zu einzelnen Verkaufsvorgängen in einer Tabelle abgelegt sind, den Gesamtumsatz ermitteln, würde man jeden einzelnen Verkaufsvorgang lesen und jeweils den Betrag zur Summe hinzu addieren. In einer spaltenorientierten Datenbank würde man einfach die Summe über die entsprechende Spalte bilden. Im Ergebnis sind beide Vorgänge zwar identisch, in der zweiten Variante werden aber andere Details des Verkaufsvorgangs nicht gelesen und somit auch nicht zur CPU transportiert. Neben solchen Optimierungsmaßnahmen auf der strukturellen Ebene der Datenbank können auch die internen Mechanismen zur Datenverwaltung und -speicherung auf die optimierte Speicherstruktur angepasst werden.

Alle Einzelmaßnahmen können in der Summe zu einer spürbaren Beschleunigung der Berechnungen führen. Faktoren von 10- bis 20-facher Beschleunigung gelten dabei als normal. In den Fachartikeln der Hersteller entsprechender Datenbanklösungen wird aber sogar von Faktoren bis zu 1.000-facher Beschleunigung – je nach Anwendung – gesprochen. In einem Fall soll sich die Verarbeitungszeit sogar von etwa drei Tagen auf zwei Sekunden reduziert haben, was einer 125.000-fachen Beschleunigung entspricht. Solche Zahlen sind mit Vorsicht zu genießen, wenn die genauen Umstände der Messung und die ergriffenen Maßnahmen nicht offen liegen. Aber selbst wenn nur ein Teil einer derartigen Beschleunigung durch die In-Memory-Technik selbst erzielt wurde, sind das zumindest Hinweise darauf,

dass sich die Umstellung einer Anwendung von konventioneller auf In-Memory-Datenbanktechnik unter Geschwindigkeitsaspekten lohnen kann.

Die Erhöhung der Verarbeitungsgeschwindigkeit ist nicht die einzige Auswirkung, die die In-Memory-Technik mit sich bringt. Auch die Dauerhaftigkeit der Speicherung wird massiv beeinflusst – sie ist nämlich ohne Weiteres nicht mehr gewährleistet, weil der aktuelle Stand der In-Memory-Datenbank nur im Hauptspeicher verfügbar ist.

Bei einer geplanten Abschaltung des Geräts oder einem Stromausfall gehen alle Informationen im Hauptspeicher verloren. Damit ist ein grundlegendes Datenbankprinzip – die Dauerhaftigkeit von Änderungen an den Daten – nicht mehr erfüllt (zu den „ACID-Kriterien" s. auch S. 20, „Nicht nur, aber auch? –NoSQL"). Das mag in Anwendungsfällen zulässig sein, in denen Daten nur in Echtzeit verarbeitet und Ergebnisse anderen Programmen unmittelbar zur Verfügung gestellt werden. In den meisten Fällen dürfte aber die dauerhafte Speicherung gewünscht und zur Wiederherstellung der jeweils aktuellen Datenbestände oder zur Dokumentation der Verarbeitung erforderlich sein. Daher wurden verschiedene Techniken entwickelt, um die Datenbestände auch über eine geplante oder ungeplante Abschaltung hinweg zu sichern. So kann die Veränderung der Daten durch das Speichern sog. „Snap shots" oder „Checkpoint images" dokumentiert werden. Dabei wird ein entsprechender Speicherauszug entweder zeitgesteuert oder anlassbezogen erstellt und gespeichert. Eine weitere Möglichkeit der Dokumentation besteht in der Speicherung der einzelnen Verarbeitungsschritte. Das hat den Vorteil, dass nicht große Datenmengen, sondern nur die ausgeführten Anweisungen festgehalten werden müssen. Um die Daten später im Speicher wiederherzustellen, müssen dann allerdings – ausgehend von einem Basisdatenbestand – alle Verarbeitungsschritte noch einmal ausgeführt werden. Neben diesen Arten der Protokollierung gibt es auch Techniken, um die Daten auf „nicht flüchtigen" Medien zu sichern. Dies kann entweder in speziellen Speicherbausteinen geschehen – sog. NVRAM (für engl. „Non Volatile Random Access Memory"). Oder es erfolgt eine kontinuierliche Datenbankreplikation auf hochverfügbare Komponenten. Schließlich gibt es auch sog. Hybrid-Ansätze für In-Memory-Datenbanken. Diese können gemäß dem Motto: „Was man nicht im Kopf hat, muss man von der Festplatte holen." Daten nicht nur im Hauptspeicher, sondern auch auf Festplatten speichern.

Die technische und konzeptionelle Ausgestaltung von In-Memory-Datenbanken erlaubt eine Vielzahl von Varianten, die sich nicht nur quantitativ, sondern auch qualitativ unterscheiden. Insofern verwundert es nicht, dass der Markt mehr Produkte zu bieten hat, als die von zwei großen Herstellern. In entsprechenden Übersichten werden 40 Produkte gelistet – mit steigender Tendenz.

BEWERTUNG

Die technischen Möglichkeiten, die im In-Memory-Computing stecken, wecken schnell Erwartungen an mehr Verarbeitungskomfort und verbesserte Auskunftsfähigkeit: Auch die Ergebnisse komplexer Analysen können künftig auf Knopfdruck fast sofort vorliegen. Doch In-Memory-Technik gibt es nicht zum Nulltarif – selbst wenn die Preise für Speicher und für Rechenleistung permanent fallen. Dagegen steigen tendenziell die anteiligen Kosten für Datenbanksoftwarelizenzen und sind meist an die steigende Prozessorleistung gebunden. Abgestimmte Geräte – sog. Appliances –, die für das In-Memory-Computing optimiert sind, stellen sehr hohe Anforderungen an Geschwindigkeit, Stabilität und Umfang der eingebauten Komponenten. Dazu können Aufwände für die Optimierung auf Anwendungsebene kommen. Vor diesem Hintergrund weisen Hersteller zu Recht darauf hin, dass man vor der Einführung der schnellen Technik auch nach der Sinnhaftigkeit der Beschleunigung fragen muss. Ist mehr möglich, als ein reines „schnelles Rechnen"? Können evtl. neue, komplexe fachliche Fragestellungen bearbeitet werden? Können neue Fragestellungen „interaktiv" und experimentell erarbeitet werden? Und wer in der Organisation kann dies tun – nur Datenbankspezialisten oder alle Fachmitarbeiter? Sowohl für privatwirtschaftliche Unternehmen wie auch für Verwaltungen sollte bei Überlegungen zum Einstieg in die In-Memory-Technik ein geschäftlicher resp. fachlicher Mehrwert im Vordergrund stehen.

Verwaltungsrelevanz: ■■□□

Umsetzungsgeschwindigkeit: ■■■■

Marktreife/Produktverfügbarkeit: ■■■■

NICHT NUR, ABER AUCH? – NOSQL

Seit rund 40 Jahren ist SQL, die strukturierte Abfragesprache (engl. Structured Query Language), das Maß aller Dinge für die Verwendung von Datenbanken. Wenn es darum geht, Daten aus einem Speicher zu befreien und in Softwareanwendungen zum Leben zu erwecken, ist SQL oft erste Wahl. Das zugrundeliegende Datenmodell basiert auf Relationen, die einzelne Informationen als Attribute eines Datensatzes zusammenfassen – z. B. die Attribute Straße, Hausnummer, Postleitzahl und Ort zu einer Adresse. Derart strukturierte Daten lassen sich sehr einfach in Tabellen ablegen und die Sprache SQL bietet das Handwerkszeug, um aus solchen Tabellen die gewünschten Informationen wieder herauszuholen und zu bearbeiten.

Jeder, der mit einem Computer arbeitet weiß, dass es neben strukturierten Daten wie Adressbuch, Dateiverzeichnis oder Kontoinformationen auch zahlreiche unstrukturierte oder wenig strukturierte Daten gibt: So lassen sich Texte und Bilder nur sehr bedingt als tabellarische Ansammlung von Attributen darstellen. Doch die Zahl und der Umfang solcher unstrukturierter Daten nimmt immer mehr zu. Internetseiten, E-Mails, Konzeptpapiere und ähnliches füllen Festplatten und andere Speichermedien immer mehr. Die Daten sind zudem zunehmend vernetzt – nicht nur im Internet, das durch Hyperlinks zu einem unendlich scheinenden Wissensspeicher geworden ist. Auch auf dem heimischen Computer lassen sich beispielsweise Mailprogramm, Kalender und Datenablage immer mehr vernetzen – auch wenn jede Anwendung evtl. über eine separate Datenhaltung verfügt. Und ein Teil der Daten befindet sich vielleicht schon „in der Cloud". Heterogene und verteilte Datenspeicher prägen zunehmend die IT-Landschaft. Damit passt aber auch das Bild von der Datenbank als einer Ansammlung evtl. sehr großer Tabellen nicht mehr, in denen alles Wissenswerte fein säuberlich in Spalten und Zeilen abgelegt ist.

Aufgrund dieser Entwicklungen haben Softwareentwickler ihr Augenmerk auf Datenbanktechniken geworfen, die der einen oder anderen dieser Herausforderungen besser gewachsen sind, als das relationale Modell und die Sprache SQL. Unter dem Namen „NoSQL" hat sich eine Entwicklungsbewegung gebildet, die verschiedene Konzepte und funktionierenden Systeme hervorgebracht hat – zumeist als Open Source-Lösung. Dabei steht „NoSQL" nicht etwa für die Aufforderung, kein SQL zu verwenden. Es ist vielmehr die Abkürzung für „Not only SQL" – zu Deutsch: „Nicht nur SQL". Es ist also durchaus legitim, auch klassische relationale Datenbanken einzubeziehen, wenn an einem NoSQL-Konzept gearbeitet wird – z. B. als Speicher für einen bestimmten Teil der Daten.

NoSQL-Datenbanken werden zumeist in die nachfolgend genannten vier Grundtypen eingeteilt, wobei in der Praxis zunehmend Mischformen entstehen:

- Sehr große Mengen einfacher Daten können in sog. **Key-/Value-Stores** gehalten werden. Hier wird unter einem Schlüssel jeweils ein einzelner Wert abgelegt. Damit ist diese Datenbankstruktur zwar nicht für die Ablage komplexer Datenstrukturen geeignet, sie erlaubt aber sehr schnelle Zugriffe auf die Daten und lässt sich gut über verschiedene Rechner verteilen.

- In **Document Stores** – auch „dokumentenorientierten Datenbanken" genannt – können dagegen wenig strukturierte Daten abgelegt werden – z. B. auch Texte mit Metadaten. Die Datensätze sind hier nicht in ein starres Tabellenschema gepresst, so dass nicht jeder Datensatz alle Attribute besitzen muss. Anfragen über bestimmte Attribute liefern daher alle Datensätze zurück, die dieses Attribut überhaupt besitzen und bei denen es auch den gewünschten Wert hat. Damit sind Document Stores auch besonders als Datenbanken für objektorientierte Systeme geeignet, in denen die Objekte verschiedener Klassen zwar gemeinsame Merkmale erben, jedoch ansonsten unterschiedliche Strukturen haben können.

- Werden oft gleichartige Operationen auf viele Datensätze angewendet, bieten sich sog. „**Wide Column**"-Strukturen an. Hier haben Datensätze zwar evtl. auch viele verschiedene Attribute, die Organisation der Daten orientiert sich aber an den Spalten der Datentabellen – also einzelnen Attributen. Dadurch wird es z. B. auch sehr einfach, ein weiteres Attribut in eine Datenbank einzufügen.

- Der vierte Ansatz speichert Daten in sog. Graphen. Diese mathematischen Konstrukte entstehen, indem Beziehungen zwischen Datensätzen nicht über einen Index dargestellt werden, sondern die Datensätze direkt miteinander verknüpft werden. Ein Stammbaum oder die Struktur einer Organisation können so einfach dargestellt werden. **Graphendatenbanken** können z. B. verwendet werden, um die Verbindungen zwischen Nutzern in Sozialen Netzwerken untereinander oder zu Gruppen abzubilden.

Allgemein gelten NoSQL-Datenbanken als leicht verteilbar und als fehlertolerant gegenüber Ausfällen von Teildatenbanken. Dazu ist die Datenhaltung oft redundant ausgelegt, wobei nicht unbedingt alle Daten auf allen Servern vorhanden sein müssen. Das erlaubt es, auch große verteilte Systeme aus einfachen Rechnern aufzubauen, so dass Investitionen in große und leistungsstarke Datenbankmaschinen nicht unbedingt notwendig sind.

Doch die beschriebene Einfachheit und Flexibilität von NoSQL-Datenbanken haben auch ihren Preis: Herkömmliche relationale Datenbanken verarbeiten Daten in Transaktionen. Eine Transaktion ist dabei eine logische Einheit von Verarbeitungsschritten, die die folgenden Eigenschaften der Verarbeitung garantiert:

- **Atomarität (Atomicity)**: In der Transaktion werden entweder alle Datenoperationen ausgeführt oder keine. D. h. wenn die Transaktion nicht vollständig abgearbeitet werden kann, muss der vorherige Zustand der Daten wiederhergestellt werden.

- **Konsistenzerhaltung (Consistency)**: Eine zuvor konsistente Datenbank muss nach der Transaktion auch wieder konsistent sein. Z. B. dürfen für eine Person nicht plötzlich zwei verschiedene Adressen geliefert werden – je nachdem wie diese abgefragt wird.

- **Isolation (Isolation)**: Verschiedene Transaktionen dürfen sich nicht gegenseitig beeinflussen.

- **Dauerhaftigkeit (Durability)**: Wurde eine Transaktion erfolgreich abgeschlossen, muss deren Ergebnis dauerhaft verfügbar sein – auch nach einem Systemausfall.

Diese „ACID"-Eigenschaften können von NoSQL-Datenbanken nicht alle gleichzeitig garantiert werden. Gerade die Konsistenz ist in stark verteilten Systemen nur schwierig sicherzustellen, so dass bei NoSQL-Datenbanken meist nur „eventuelle Konsistenz" garantiert wird. Das bedeutet, dass die Konsistenz erst nach einer hinreichend langen Wartezeit erreicht ist, in der keine weiteren schreibenden Aktionen erfolgen dürfen. Mit anderen Worten: Alle Transaktionen müssen abgeschlossen sein.

Für NoSQL-Datenbanken wird daher oft an Stelle der „scharfen" ACID-Eigenschaften von Verarbeitungsschritten oft nur das BASE-Prinzip gefordert. „BASE" steht für:

- **Basically Available**: Nicht jedes Datum steht immer und überall zu Verfügung, kann aber nach einer entsprechenden Wartezeit „beschafft" werden – z. B. von einem anderen Rechner.

- **Soft State**: Nicht jede Veränderung der Daten wird dauerhaft gespeichert. Nur wenn die neue Information regelmäßig aufgefrischt wird, ist sie verfügbar. Dies kann z. B. dann sinnvoll sein, wenn zeitlich veränderbare Zustandsdaten verarbeitet werden: Gibt es keine neue Meldung, wird ein „Basiszustand" angenommen.

- **Eventualy Consistent**: die oben beschriebene Konsistenz nach einer Wartezeit.

NoSQL-Datenbanken sind kein Allheilmittel für alle Datenbankherausforderungen moderner Anwendungen. Auch ist nicht jedes NoSQL-Modell für jede Systemarchitektur gleichermaßen geeignet. Deshalb verschmelzen verschiedene Ansätze in einigen Produkten miteinander und auch die Annäherung zwischen NoSQL-Konzepten – insbesondere Skalierbarkeit und Geschwindigkeit – und klassischen relationalen Datenbanken – Abfragesprache SQL und ACID-Eigenschaft – wird unter dem Stichwort NewSQL untersucht.

Für die künftige Gestaltung von Anwendungen, die große Datenmengen verarbeiten, ist es jedoch wichtig zu wissen, dass die verschiedenen NoSQL-Ansätze aus der Praxis entstanden sind und nicht allein auf Gedankenspielen zur Datenbanktheorie basieren. Mit der Entwicklung von Cloud-Strukturen und verteilten Anwendungen, die Infrastrukturen und Software als Dienste benutzen, werden neue Datenbankkonzepte an Bedeutung gewinnen.

BEWERTUNG

Öffentliche Verwaltungen verfügen in der Regel über große Datenbestände – sowohl an strukturierten als auch an wenig strukturierten Daten. Neben der Verpflichtung zur reinen Aufbewahrung besteht auch hier vielfach der Wunsch, die vorhandenen Informationen zu nutzen. Mit zunehmender Diversifizierung von Datenquellen und Datenarten ist dazu vielfältigeres Werkzeug erforderlich als relationale Datenbanken und Mechanismen zur Volltextsuche. Die Ansätze der NoSQL-Bewegung bieten hier evtl. Lösungen für neue Fragestellungen. Aufgrund der unterschiedlichen Konzepte und der entstehenden Mischformen muss im Einzelfall geprüft werden, welche Lösung für einen konkreten Anwendungsfall geeignet ist.

Verwaltungsrelevanz: ■■■□

Umsetzungsgeschwindigkeit: ■■■□

Marktreife/Produktverfügbarkeit: ■■■■

03_ GESELLSCHAFT

AMBIENT SOCIAL NETWORKING

Soziale Netzwerke sind seit geraumer Zeit am Markt etabliert. Das „Soziale" der Netzwerke zielt dabei auf ein geselliges und gesellschaftliches Miteinander rund um gemeinsame Interessen und Themen. Die Vernetzung mit „Freunden" wird dabei von den Netzwerkbetreibern gerne gefördert, denn durch immer mehr Mitglieder mit gemeinsamen Interessen können sie stärker zielgerichtet Werbung in ihren Angeboten platzieren. Das ist – neben Mitgliederbeiträgen – eins der wenigen Geschäftsmodelle, die sich für solche Netzwerke etabliert haben. Und auf welch wackeligen Beinen dieses Geschäftsmodell steht, zeigt die Berg- und Talfahrt des Aktienkurses des weltweit größten sozialen Netzes.

Schon lange gibt es in sozialen Netzwerken Vorschläge für neue Kontakte zu Bekannten von Freunden. Auch Vorschläge aufgrund regionaler Bezüge sind etabliert: „Diese Personen aus ... könnten Sie kennen!" 2009 erschienen Netzwerke, die sich über Beziehungen zu Orten – und damit indirekt zu weiteren Besuchern dieser Orte – definierten. Das Aufsuchen eines Ortes wird dabei anhand der Koordinaten eines mobilen Gerätes erkannt. Beim „Check-in" an registrierten Orten wie Hotels, Geschäften, öffentlichen Einrichtungen oder auch privaten Häusern werden dann automatisch entsprechende Kurzmitteilungen verschickt, die es anderen Nutzern dieser Dienste erlauben, Kontakt aufzunehmen und sich spontan zu treffen.

Beim diesjährigen Musik-, Film- und Medienfestival „South by Southwest" (SXSW) in Texas wurden einige mobile Anwendungen vorgestellt, die eine neue Art der sozialen Vernetzung ermöglichen. Dazu werden anhand der Interessen und des Aufenthaltsortes des Nutzers – der über die GPS-Koordinaten des Handys ermittelt werden kann – potenziell interessante Gesprächspartner in der Umgebung angezeigt. „Umgebung" bedeutet dabei nicht wie bei manch anderem georeferenzierten Dienst „mehrere Kilometer" sondern gerade einmal gut 45 Meter (50 Yards à 0,9144 m). Im Unterschied zu den oben genannten ortsbezogenen Diensten ist es hier also nicht der Veranstaltungsort an sich, über den hier die Vernetzung läuft, sondern es sind der geografische Aufenthaltsort der einzelnen Personen und deren gemeinsame Interessen.

Drei Eigenschaften charakterisieren die neuen Dienste: sie sind sozial, lokal und mobil, was zu der Abkürzung „SoLoMo" (engl. „social, local, mobile") geführt hat. Eine praktische Anwendung solcher Dienste wird beispielsweise darin gesehen, dass in Vergessenheit geratene Namen oder weitere Informationen zu anwesenden Personen relativ einfach in Erinnerung gerufen werden können. Ob sie allerdings dazu führen, wildfremde Menschen allein aufgrund gemeinsamer Interessen anzusprechen und sich mit ihnen zu vernetzen, mag fraglich erscheinen. Im Rahmen von Messen, Partys oder zum Auffinden von Bekannten in anderen Menschenansammlungen mag das möglich sein.

Damit Social Ambient Networking gut funktionieren kann, muss zum einen die Anzahl der Mitglieder möglichst groß sein. Zum anderen müssen genügend potenzielle Interessen veröffentlicht werden, wenn man „gefunden" werden möchte. Auch wenn man gegebenenfalls die Weitergabe der Informationen auf direkte „Freunde" oder auch deren Bekannte beschränken kann, drängen sich hier Fragen des Datenschutzes auf. Denkbar wäre beispielsweise ein Missbrauch durch das Erstellen von „Phantomprofilen" mit sehr vielen Interessen, um damit Menschen in der Umgebung auszuspionieren.

Durch die Integration von Social Ambient Networking-Diensten oder –Funktionen in bestehende Geschäftsnetzwerke oder in Anwendungen für das Kundenmanagement (englisch: „Customer Relationship Management", CRM) könnte Kundenpflege – gerade bei Messen und anderen Veranstaltungen – möglicherweise wesentlich vereinfacht werden. Dies wäre ein weiterer Anknüpfungspunkt für eine stärkere Integration von Sozialen Medien und Kundenmanagement, die sich unter der Bezeichnung „Social CRM" als weiterer aktueller Trend abzeichnet. Eventuell ließen sich so auch tatsächlich neue Geschäftsmodelle für Soziale Netzwerke entwickeln.

BEWERTUNG

Ernsthafte Anwendungen für Ambient Social Networking zeichnen sich erst ganz zaghaft ab. Wie bei vielen Themen rund um soziale Netzwerke besteht auch hier die große Herausforderung darin, den besten Mittelweg zwischen Offenheit und Datenschutz zu finden. Informationen, die man in einem Zusammenhang bekannt geben möchte, um das Knüpfen von Kontakten zu vereinfachen, sollen in einem anderen Zusammenhang möglicherweise verborgen bleiben. Da durch die Nutzung von Ambient Social Networking-Diensten zunächst einmal signalisiert wird, dass man an Kontakten interessiert ist, werden Einstellungen zur Privatsphäre und gegebenenfalls die Nutzung verschiedener Profile auf dem Weg zum zielgerichteten Einsatz eine wichtige Rolle spielen. Derzeit sind die Anbieter aber noch mehr damit befasst, die grundlegenden Funktionen ihrer Netzwerke weiterzuentwickeln, als dass sie auf das Thema Datenschutz viel Augenmerk richten würden. Solange dürften die Dienste auch eher im spielerischen und experimentellen Bereich genutzt werden.

Verwaltungsrelevanz: ■□□□

Umsetzungsgeschwindigkeit: ■■■■

Marktreife/Produktverfügbarkeit: ■■■■

DIGITAL NATIVES – SELBSTVERSTÄNDLICH DIGITAL

Wer von uns, der diesen Bericht schreibt oder liest, hatte wohl in seiner Kindheit als Berufswunsch „Firewall-Spezialist", „Web-Designer" oder „Social-Media-Experte" angegeben? Abgesehen davon, dass in diesem Alter die schicken Anzüge und Autos von Feuerwehr oder Müllabfuhr auf kleine Kinder viel anziehender wirkten als eine Tätigkeit am Computer, gab es diese Berufe seinerzeit noch nicht. Die Schule steckt auch heute in dem Dilemma, Kinder und Jugendliche für Berufe (aus)bilden zu müssen, die es eventuell noch gar nicht gibt – und das mit den Methoden von heute oder gestern. Ein möglicher Bestandteil von modernem Unterricht ist der Einsatz von neuen Techniken und Medien. Das Internet hat auch hier ganz neue Herausforderungen geschaffen, wie aktuelle Diskussionen um Plagiate zeigen. Der Umgang mit diesen neuen Elementen wird zum Teil dadurch erschwert, dass im Klassenzimmer – aber auch später in der weiteren Ausbildung – die sog. Digital Natives, also Menschen, die mit Computer und Internet aufwachsen beziehungsweise aufgewachsen sind, auf die älteren sog. Digital Immigrants treffen, die die Verbreitung von Computern und Internet als „Volkstechniken" erst im Erwachsenenalter miterlebt haben.

Über die vermeintlichen Besonderheiten der Digital Natives ist viel gesprochen und geschrieben worden. Inzwischen setzt sich aber immer mehr die Erkenntnis durch, dass die „jungen Leute" zwar die neuen Techniken und Medien viel selbstverständlicher und häufiger einsetzen als zum Beispiel ihre Eltern oder Lehrer, dass sie aber deswegen nicht unbedingt mehr von den inneren Zusammenhängen verstehen. Dass Jugendliche mit Computer und Smartphone Dinge vermögen, die Erwachsene in Staunen versetzen, bedeutet nicht, dass diese Generation insgesamt schlauer ist als andere. Die amerikanische Wissenschaftlerin Danah Boyd sagt dazu: „Das Internet hat nichts Magisches mit einer ganzen Generation von Jugendlichen gemacht. Es hat sie nicht schlau gemacht, aber auch nicht dumm." Und genauso wenig, wie nicht jeder, der ein Auto fährt, auch in der Lage ist, dieses bei einem Schaden zu reparieren, sind die Digital Natives in der Lage zu programmieren, Netzwerke zu konfigurieren oder technische Systeme zu bauen. Sie sind aber oft in der Lage, die neuen Techniken und Medien ganz selbstverständlich und – für „Außenstehende", also die Digital Immigrants – recht virtuos zu nutzen. So selbstverständlich wie noch vor einigen Jahren Telefon und Fax die Mittel der schnellen Geschäftskommunikation waren oder mittlerweile E-Mail verwendet wird, nutzen sie heute soziale Netzwerke und Kurznachrichtendienste. Schrieb die Generation der Großeltern und Eltern noch mehr oder weniger selbstverständlich ein Tagebuch, so sind es heute Webseiten und Blogs. Und Handys oder Smartphones sind seit der Verbreitung der SMS bei vielen Jugendlichen ständige Begleiter.

Die Selbstverständlichkeit, mit der die jüngeren Generationen Internet, soziale Medien und moderne Technik nutzen, hat auch Auswirkungen auf ihre Erwartungen an die Arbeitswelt. Spätestens im Zusammenhang mit „Bring your own Device" (BYOD), ist viel über diese Erwartungen und deren Auswirkungen geschrieben worden. Auf dem Computer am Arbeitsplatz keine sozialen Netze nutzen zu dürfen, ist für diese Generation genau so irritierend, als müsste man beim Betreten des Büros seinen eigenen Kugelschreiber abgeben und stattdessen mit einem standardisierten Holzbleistift der Stärke HB schreiben.

Die Selbstverständlichkeit der Techniknutzung hat aber auch noch ein andere Folge: Die spezifischen Sicherheitsanforderungen einer hoch technisierten Arbeitswelt werden nicht unbedingt erkannt bzw. akzeptiert. So ist ein Argument der BYOD-Befürworter, dass jüngere Mitarbeiter „sowieso" ihre eigenen Geräte mit ins Unternehmen bringen und dort einsetzen – auch wenn dies seitens des Arbeitgebers nicht vorgesehen ist. Daneben ergab eine Analyse von 70 Millionen Passwörtern, dass diese bei jungen Menschen unter 25 Jahren nur halb so sicher sind wie die Passwörter von Menschen über 55 Jahren – gemessen am Aufwand für einen „Brute Force"-Angriff durch Ausprobieren. Dass die Selbstverständlichkeit der Nutzung von Internet und Co. einen negativen Einfluss auf Sicherheitsbelange haben kann, wird auch durch ein weiteres Ergebnis der Analyse gestärkt: Diejenigen Nutzer, die Kreditkartendaten in ihren Online-Accounts hinterlegt hatten – die also das Internet auch zum Erwerb von kostenpflichtigen Leistungen nutzen –, hatten oft nur wenig sichere Passwörter gewählt.

Auch in anderer Hinsicht pflegen Digital Natives einen eher unbekümmerten Umgang mit IT-Sicherheit: Eine internationale Befragung ergab, dass junge Nutzer der Altersgruppe 18-25 Jahre dazu neigen, Sicherheitsmechanismen wie Firewalls zu deaktivieren, wenn diese die Benutzung von Online-Spielen oder Sozialen Netzen behindern.

So wundert es nicht, wenn in der Presse die rhetorische Frage gestellt wird, ob die Digital Natives ein Sicherheitsrisiko für Unternehmen darstellen. Nicht nur wegen der viel zitierten demografischen Entwicklung wird diese Frage dann verneint. Die einschlägigen Beiträge sehen die junge Generation eher als Chance und Herausforderung für die Belebung der Arbeitswelt. Der Pädagoge Marc Prensky, der den Begriff „Digital Naives" prägte, fordert daher mehr auf die jungen Generationen zu hören und auf deren Bedürfnisse einzugehen. Auf die IT übertragen kann man dies als die Aufforderung verstehen, die IT so sicher zu machen, dass ein angemessener Umgang mit neuen Medien und Techniken möglich ist. Es kann jedoch nicht bedeuten, alle Sicherheitsmechanismen über Bord zu werfen – weder die technischen noch die organisatorischen.

BEWERTUNG

Die Digital Natives halten auch in den Verwaltungen Einzug. Neben den technischen bringt dies auch fachlich inhaltliche Herausforderungen mit sich, da hier Themen wie Datenschutz oder Vertraulichkeit einen anderen Stellenwert einnehmen, als es die Digital Natives gewohnt sind. Dass sich die öffentlichen Verwaltungen langsam verändern, kann man an der Open Government-Bewegung (s. auch S. 26, „Offen in alle Richtungen – Open Government") sehen. Auch hier wird es – wie überall – wichtig sein, den angemessenen Kompromiss zwischen den Erwartungen der Digital Natives und den Rahmenbedingungen einer öffentlichen Verwaltung zu finden.

Verwaltungsrelevanz: ■■■□

Umsetzungsgeschwindigkeit: –

Marktreife/Produktverfügbarkeit: –

„LASST DIE SPIELE BEGINNEN" – GAMIFICATION

Eine der bekanntesten Episoden aus den Abenteuern des Tom Sawyer handelt davon, dass Tom als Strafarbeit den Zaun seiner Tante Polly streichen soll. Den anderen Jungen, die vorbei kommen, erklärt er, dass das Streichen eine besonders anspruchsvolle Arbeit sei, die nicht jeder erledigen könne. Damit weckt Tom bei den Jungen den Wunsch, mit streichen zu dürfen. Nach und nach tauschen sie verschiedene „Schätze" gegen die Erlaubnis, ein paar Bretter anzumalen.

In dieser Geschichte geht es letztendlich um die Verstärkung eines Verhaltens – hier das Zaunstreichen – durch eine in Aussicht gestellte Belohnung – die Anerkennung, eine besondere Leistung vollbringen zu können. Diese positive Verstärkung, die auch eingesetzt wird, wenn ein Hund für einen Trick mit einem „Leckerli" belohnt wird, ist eine von mehreren Möglichkeiten, ein bestimmtes Verhalten zu fördern beziehungsweise zu unterdrücken. Die Bestrafung – zum Beispiel das „Knöllchen" für zu schnelles Fahren – ist eine weitere Möglichkeit.

Um derlei Feedback-Mechanismen geht es, wenn von „Gamification" oder – seltener gebraucht – „Spielifizierung" die Rede ist. Die Idee dabei ist, Arbeit oder andere ernste Tätigkeiten durch spielerische Elemente attraktiv zu machen und bestimmte Verhaltensmuster zu verstärken. Dies lässt sich besonders einfach in einem IT-gestützten Umfeld realisieren. Auf dem Computer gibt es solche Elemente schon lange: Der „Fortschrittsbalken" für langanhaltende Operationen ist zwar noch kein Spiel-Element im engeren Sinne, er verstärkt aber die Geduld des Anwenders, indem er die Ungewissheit über das Ende der Aktion beseitigt („negative Verstärkung").

Das andere Extrem der verspielten Gestaltung sind Hilfefunktionen beziehungsweise Trainingsprogramme, die sich vollständig als Spiel präsentieren: Durch das Abarbeiten von „Spielebenen" lernt der Benutzer die Funktionen der eigentlichen Software kennen und anzuwenden.

Ein weit verbreitetes Elemente aus der Spielewelt, das zunehmend in anderen Anwendungen eingesetzt wird, sind kleine Preise in Form von „Abzeichen" (engl. „Badges"), die für das Erreichen eines Zwischenziels verliehen werden. Ein Beispiel dafür sind die Badges von foursquare, einem standortbezogenen sozialen Netzwerk: Hier werden Badges für das mehrmalige Aufsuchen eines registrierten Ortes und weitere Aufgaben verliehen. Etwas ernsthafter werden Badges und weitere Belohnungen in der Projektmanagementsoftware RedCritter Tracker eingesetzt. Diese können Personen oder Teams erhalten, die bestimmte Projektaufgaben erledigt haben.

Auch ohne IT lassen sich Alltagsaufgaben spielerisch gestalten und dadurch attraktiver machen. So wurden zur besseren körperlichen Ertüchtigung Fußgänger dazu animiert, die Treppe anstelle einer Rolltreppe zu verwenden, indem deren Stufen in eine Klaviatur umfunktioniert wurden. Beim Betreten der Stufen erklangen Töne. Durch ein paar Zusatzschritte ließen sich auch Melodien spielen. Die Benutzung der Treppe gegenüber der Rolltreppe erhöhte sich um 66 Prozent.

Gamification soll dazu beitragen, das Verhalten von Menschen positiv zu beeinflussen, indem es mehr Spaß macht, bestimmte Dinge zu tun. Was dabei „positiv" ist, hängt allerdings vom Betrachter ab. Wenn durch spielerische Elemente das Kaufverhalten potenzieller Kunden beeinflusst wird, kann dies sowohl positiv als auch negativ gesehen werden. Darüber hinaus können sich die zunächst positiven Effekte umkehren, wenn bestimmte Aufgaben nur noch in dem Maße erledigt werden, das notwendig ist, um eine Belohnung zu erhalten, ohne dabei die erforderliche Qualität zu erhalten. Werden Belohnungen sehr umfassend eingesetzt, kann das auch dazu führen, dass eigentlich selbstverständliche Aufgaben nicht mehr erledigt werden, wenn sie nicht zu Punkten, Preisen oder Auszeichnungen beitragen. Und schließlich ist zu bedenken, dass vermeintliche Belohnungen bei verschiedenen Menschen eine unterschiedliche Bedeutung haben können. So wäre für einen Anwender einer Software „XY" die Auszeichnung „XY-Power-User" eher eine Bestrafung, wenn er eigentlich Anhänger eines alternativen Produkts ist.

BEWERTUNG

Öffentliche Verwaltungen tun sich schwer mit der Belohnung von positivem Verhalten, da der positive Fall in der Regel der – oft durch Gesetze und Vorschriften geregelte – Normalfall ist. Lediglich die Sanktionierung von negativem Verhalten durch erhöhte Gebühren und ähnliches ist weit verbreitet. Der Fall einer Geschwindigkeitslotterie dürfte daher eher die Ausnahme bleiben: Bei dieser Lotterie nahmen Autofahrer, die die korrekte Geschwindigkeit einhielten, an einer Verlosung teil. Doch auch wenn gesetzliche Bestimmungen derartigen „echten" Belohnungen im Weg stehen, lohnt es sich eventuell über spielerische Anreizsysteme auch für E-Government-Anwendungen nachzudenken.

Verwaltungsrelevanz: ■□□□

Umsetzungsgeschwindigkeit: ■■■■–■■■□

Marktreife/Produktverfügbarkeit: –

OFFEN IN ALLE RICHTUNGEN – OPEN GOVERNMENT

Die Offenheit von Verwaltungen ist zurzeit ein Thema, das viele Menschen bewegt. Einen wesentlichen Anschub hat es dadurch erhalten, dass der amerikanische Präsident von Anfang seiner Amtszeit an „Open Government" durch eine entsprechende Direktive in sein Regierungsprogramm aufgenommen hat. Darin steht „Offenheit" für die drei Handlungsfelder: Transparenz von, öffentliche Teilhabe an und Zusammenarbeit mit Verwaltung. Diese Charakterisierung zeigt, dass Open Government zunächst ein politisches bzw. verwaltungsorganisatorisches Thema ist. Da bei dessen Umsetzung aber IT insgesamt – und die Techniken des Web 2.0 im Besonderen – eine wichtige Rolle spielen, handelt es sich durchaus auch um ein Trendthema in der IT mit deutlichen Auswirkungen auf die Verwaltung. Um diese Auswirkungen genauer analysieren zu können, sollen aber zunächst noch die genannten Handlungsfelder ein wenig genauer betrachtet werden. Dabei ist zu bedenken, dass der englische Begriff „Government" – auch im Zusammenhang mit „E-Government" – stärker das Regieren einbezieht, als es im deutschen Begriff „Verwaltung" zum Ausdruck kommt. Dies ist deshalb wichtig, weil die Handlungsfelder Teilhabe von und Zusammenarbeit mit der Öffentlichkeit – also mit Bürgerinnen und Bürgern, aber auch Unternehmen und Verbänden – nur da mit Leben gefüllt werden können, wo angemessene Spielräume dafür bestehen. Und solche Spielräume sind eher da zu finden, wo nicht zu viele rechtliche und organisatorische Regelungen detaillierte Vorgaben machen.

„Teilhabe und Zusammenarbeit" ist auch das Mantra der Web 2.0-Gemeinde, die nicht umsonst vom „Mitmachweb" spricht: Jeder steuert Inhalte bei, was wiederum mit dem Handlungsfeld „Transparenz" korrespondiert, arbeitet an anderen Inhalten und ggf. in den dahinterliegenden Prozessen mit – „Teilhabe" – und schließlich können aus bereitgestellten Informationen, Diensten und Anwendung neue Produkte entstehen – „Zusammenarbeit". Dies weckt hohe Erwartungen an ein Government 2.0 und damit auch an Politik und Verwaltung, die sich dank neuer Webtechniken öffnen. In den einschlägigen Veröffentlichungen zu Open Government wird dann auch schnell der Werkzeugkasten des modernen Internet ausgebreitet und es werden mehr oder weniger überzeugende Beispiele präsentiert, wie mit diesen Werkzeugen Offenheit hergestellt wird. Das Angebot der Informationsdienste, die von Verwaltung und Politik genutzt werden können, ist groß. Es reicht von klassischen Portalen mit Feedback-Funktion über Blogs – einschließlich Foto-, Audio- und Video-Podcast sowie Microblogs wie Twitter – über Wikis bis hin zu Foren. Stellt man aber die Frage nach den Inhalten für diese Dienste und Anwendungen, zeigt sich schnell, dass nur wenige davon den Verwaltungen und Politik tatsächlich neue Möglichkeiten eröffnen. Während die Politik noch von den schnellen Möglichkeiten, sich zu präsentieren und mit anderen auszutauschen, profitieren kann, ist dies bei klassischen Verwaltungen schon schwieriger. Die Veröffentlichung von Daten und Informationen aus der Verwaltung kann zwar wesentlich zur deren Transparenz – und damit letzten Endes zur Transparenz bei der Umsetzung von Politik – beitragen. Das eigentliche Verwaltungshandeln liefert aber meist nur wenig Stoff für ein spannendes Blog oder Ähnliches. Und die Investition einer Behörde in einen solchen Dienst lohnt sich nur dann, wenn die zur Verfügung gestellten, aktuellen Informationen auch gelesen werden. Dies gilt auch für die Investition in die Bereitstellung offener Daten. Hierbei geht es nicht darum, Informationen zu verbreiten, die ggf. auch schon an anderer Stelle zur Verfügung stehen. Transparenz wird nur dann erzeugt – und kann somit zum Vertrauen in die Verwaltung beitragen –, wenn es sich um neue und wichtige Informationen handelt. Und so lautet eine der Anweisungen in der US-amerikanischen Direktive zu Open Government auch, dass jede (US-amerikanische) Bundesbehörde binnen 45 Tagen drei Bereiche von hochwertigen und nicht bereits anderweitig im Web zur Verfügung gestellten Daten identifizieren und veröffentlichen soll. Daneben soll Bürgerinnen und Bürgern die Möglichkeit für Feedback, für eine Priorisierung zu veröffentlichenden Informationen und zur Stellungnahme zum Open Government-Plan der Einrichtung gegeben werden. Und schließlich wird auch noch gefordert, auf derlei öffentliche Mitteilungen zu reagieren.

Solche Feedbackschleifen sind aber nicht nur im Zusammenhang mit Transparenz von Verwaltung wichtig. Noch wichtiger wird die Rückkopplung im Hinblick auf Teilhabe und auf Zusammenarbeit. Hier muss allen Beteiligten vermittelt werden, dass einerseits ihre Anregungen und Beiträge ernst genommen werden und in die weitere Gestaltung öffentlichen Handelns tatsächlich einfließen, und dass andererseits die Zusammenarbeit mit ihnen auch gewürdigt wird. Doch die dafür notwendigen Spielräume in Verwaltungsabläufen sind durch rechtliche, politische, finanzielle, organisatorische und andere Rahmenbedingungen sehr begrenzt und müssen dann erst anhand von Gesetzen und Regelungen – und dafür notwendig durch politischen Willen – geschaffen werden.

So ist es nicht verwunderlich, dass im Hinblick auf Teilhabe und Mitarbeit immer wieder die gleichen Beispiele für Webanwendungen des Open Government angeführt werden. Dies sind zum einen Meldedienste für Mängel im öffentlichen Raum. In einer Kombination von Geo- und Kartendienst mit Fotoportal und Kommentierungs- oder gar Diskussionsfunktion können Bürgerinnen und Bürger Hinweise auf Mängel und Probleme geben. Dies können z. B. Verkehrsprobleme, ungünstige Öffnungszeiten, Defekte an Einrichtungen oder wilde Müllkippen sein. Hier bietet sich – vorwiegend kommunalen – Verwaltungsstellen die Möglichkeit der schnellen Verbesserung bzw. Beseitigung. Eine Eingabe seitens der Bevölkerung kann also tatsächlich einen Verwaltungsvorgang initiieren. In einem entsprechenden Feedback kann die zuständige Stelle den Bearbeitungsstand mitteilen oder ggf. darüber informieren, warum ein Thema nicht verfolgt werden kann.

Zum anderen werden immer wieder sog. Bürgerhaushalte als Beispiel für Open Government genannt. Hier sind Bürgerinnen und Bürger ohne politisches Mandat gehalten, über die Verwendung von freien Haushaltsmitteln in – auch wieder vorwiegend kommunalen – Haushalten mit zu beraten und ggf. auch mitzuentscheiden. Die Erfahrungen damit sind allerdings nicht immer positiv. Z. B. kann eine geringe Beteiligung an den entsprechenden Verfahren dazu beitragen, dass solche Initiativen wieder eingestellt werden. So hatte die Stadt Wiesbaden aufgrund einer Beteiligung bei der Planung des Bürgerhaushalts 2010/2011 von weniger als 2 % der Bevölkerung beschlossen, die dafür vorgesehenen Mittel von jeweils einer Million Euro den Schulen und Ortsbeiräten zugutekommen zu lassen. Ob bei derartigen Verfahren eine zunehmende Online-Präsenz aller Beteiligten zu mehr Akzeptanz und Mitwirkung führt, muss sich zeigen.

Moderne Informationstechnik kann ein Motor der offenen Verwaltung sein. Ohne zeitnahe Bereitstellung von Informationen und ohne die Möglichkeit, auf einfache Art an öffentlicher Verwaltung teilzuhaben, verlaufen die Open Government-Bemühungen schnell im Sande. Dabei muss man sich aber auch vor Augen führen, dass es bei der Öffnung von Verwaltungen und deren Daten nicht allein um Transparenz sondern auch um Wirtschaftsgüter geht: Die Forderung nach maschinenlesbaren Informationen hat nicht allein zum Ziel, Informationen auf den modernen Vertriebskanälen 1:1 zu verbreiten. Es geht dabei auch um die Möglichkeit, auf Basis dieser Daten neue Anwendungen und Dienste entwickeln und am Markt anbieten zu können.

Elektronische Unterstützung von Teilhabe und Zusammenarbeit kämpft aber auch mit spezifischen Herausforderungen. So müssen Mittel und Wege der Beteiligung gefunden werden, die einerseits dem Datenschutz genügen – z. B. durch anonyme Beteiligung. Auf der anderen Seite sollte aber auch sichergestellt werden, dass nicht einzelne Personen oder Gruppen durch mehrfache Beteiligung an einer Sache deren Ausgang einseitig verändern. Die Spielregeln der elektronischen Demokratie müssen sich erst noch herausbilden. Das Potenzial ist vorhanden und die IT-Werkzeuge auch. Über deren angemessenen Einsatz wird die Geschichte entscheiden.

BEWERTUNG

Die Hoffnungen, die derzeit in Open Government gesetzt werden, stellen die Verwaltungen – wie auch Regierungen und Politik allgemein – vor große Herausforderungen. Dazu gehört es insbesondere, innerhalb der bestehenden rechtlichen, organisatorischen, finanziellen, politischen und weiterer Rahmenbedingungen die neuen Techniken kreativ einzusetzen und ggf. bessere Rahmenbedingungen zu schaffen. Dadurch können sowohl Verwaltung als auch Bürgerinnen und Bürger, Wirtschaft bzw. Organisationen einen Nutzen von Open Government haben.

Verwaltungsrelevanz: ■■■■

Umsetzungsgeschwindigkeit: ■■■□

Marktreife/Produktverfügbarkeit: ■■■□

04_ SICHERHEIT

SICHERHEIT IM CYBERSPACE?

Wer im Zusammenhang mit IT an Sicherheit denkt, hat oft die Gefahren vor Augen, die aus dem Internet drohen. Viren und Trojaner, Phishing und Code Injection, Man in the Middle-Angriff und Drive By-Malware sind nur einige Schlagworte, denen man dabei begegnet. Doch es sind nicht allein die Gefahren aus dem Internet, die jährlich in Deutschland Millionenschäden anrichten. Laut einer Studie belaufen sich diese hier allein bei Unternehmen auf knapp fünf Millionen Euro. Nach einer anderen Untersuchung wird der Gesamtschaden durch Internetkriminalität in Deutschland sogar auf 16 Milliarden Euro geschätzt.

Zunehmend werden auch IT-Systeme bedroht, die nicht – oder nicht permanent – mit offenen Netzen verbunden sind. Die Angriffe gelten Systemen, die im gesamten virtuellen Raum, dem sogenannten „Cyberspace" verteilt sind. Darum wird heute auch oft von „Cybersicherheit" gesprochen. Der Begriff „Cyber" leitet sich vom altgriechischen Wort für Kybernesis, die Steuerung im wörtlichen Sinne, ab und wurde schon früh auf die Steuerung von Maschinen und Computern bezogen.

Liegt der Fokus mehr auf Bedrohungen, spricht man auch von „Cyberkriminalität", „Cyberkrieg" oder „Cyberterrorismus". Die letztgenannten Begriffe machen deutlich, dass die Stellen die sich mit der Abwehr solcher Gefahren für die IT- und Kommunikationsinfrastruktur befassen, mit mehr zu kämpfen haben als mit virtuellen Lausbubenstreichen oder dem Freizeitvergnügen von Hackern, die einen Sport daraus machen, vermeintlich sichere Systeme zu knacken. Die Stellen, die sich mit der „Cyberabwehr" befassen, gehen viel mehr davon aus, dass organisierte Kriminalität mit hoher Energie hinter vielen Angriffen steckt. Insbesondere im Zusammenhang mit Wirtschaftsspionage wird sogar davon ausgegangen, dass Angriffe aus dem und auf den Cyberspace auch von fremden Staaten gesteuert werden.

Doch wie sind Angriffe auf Systeme möglich, die nicht mit dem Netz verbunden sind? Sofern das Zielgerät eines geplanten Angriffs nicht zugänglich ist, setzen die Angreifer darauf, dass kaum eine IT-Komponente ihr ganzes virtuelles Dasein losgelöst von jeglichem anderen Gerät fristet. Früher oder später findet ein Datenaustausch statt – zum Beispiel im Rahmen von Wartungsarbeiten. Wenn ein Schadprogramm dann zumindest im Arbeitsumfeld des Zielgerätes eingeschleust werden kann, ist die Wahrscheinlichkeit hoch, dass der Schädling das Ziel auch erreicht. So gelang es zum Beispiel den hoch spezialisierten Computerwurm Stuxnet in Steuerungsrechnern iranischer Atomanlagen zu platzieren.

In dem „früher oder später" steckt auch noch ein neuer Aspekt von Cyberangriffen: Viele herkömmliche Angriffe setzen auf Masse und versuchen, innerhalb kurzer Zeit Sicherheitslücken an vielen Stellen auszunutzen. Die Sabotage von Servern durch Denial of Service-Angriffe zielt sogar gerade darauf ab, durch möglichst viele parallele Anfragen

das Zielsystem in die Knie zu zwingen. Auch wenn sich solche Angriffe nur bedingt abfangen lassen, so sind sie in der Regel zumindest sehr gut dadurch erkennbar, dass ungewöhnliche Vorgänge plötzlich und in großer Zahl auftreten.

Moderne Angriffe verhalten sich oft vergleichsweise still. So wird zwischen der Infektion eines angegriffenen Systems und weiteren Aktivitäten immer wieder eine größere Pause eingelegt. Dadurch wird es für Sicherheitssysteme sehr schwierig, die einzelnen Veränderungen im System mit einander in Verbindung zu bringen und als einen Angriff zu identifizieren. 2011 wurde ein Hackerangriff entdeckt, der seit 2006 Daten von mindestens 72 Rechnern aus der Privatwirtschaft, von Organisationen und Regierungseinrichtungen gestohlen hatte. Auch hier kursierte die Vermutung, dass der Angriff von staatlicher Seite gesteuert wurde. Dass Staaten sich nicht nur mit der Cyberabwehr befassen, sondern aktiv in das Thema „Cyberangriffe" verwickelt sind, wurde spätestens klar, als der US-amerikanische Verteidigungsminister von der Erstschlagfähigkeit im Cyberkrieg sprach.

Neben der zeitlichen Streckung von Cyberangriffen erschwert auch deren räumliche Verteilung die Abwehr. So gelten insbesondere verteilte Infrastrukturen wie Strom- oder Datennetze als kritisch, da sie an vielen Stellen angreifbar sind. Zudem sind die Zuständigkeiten für Schutzmaßnahmen oft auf viele Schultern verteilt. In großen Organisationen ist daher ein koordiniertes Vorgehen gegen Cyberangriffe von großer Bedeutung. Auch im staatlichen Bereich spielt die Abstimmung der verschiedenen Ebenen und der verschiedenen Ressorts eine wichtige Rolle, wenn es um den Schutz übergreifender kritischer Infrastrukturen geht. Daher wurden Gremien und Einrichtungen wie die Bund-Länder-Arbeitsgruppe Cybersicherheit oder das Nationale Cyber-Abwehrzentrum geschaffen, die das Thema Cybersicherheit organisationsübergreifend bearbeiten. Im Nationalen Cyber-Sicherheitsrat findet zudem die Vernetzung mit der Privatwirtschaft statt. Auch auf Länderebene wurden entsprechende Gremien eingerichtet, wie zum Beispiel die hessische Kompetenzstelle Cybersicherheit. Auf Bundesebene definieren die „Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)" und der „Nationale Plan zum Schutz der Informationsinfrastrukturen" die Ziele und Grundlagen der übergreifenden Strategie zur IT-Sicherheit. Dabei wird auf Prävention, Reaktion und Nachhaltigkeit gesetzt und der kooperative Ansatz unter Beteiligung aller relevanten Partner festgeschrieben.

BEWERTUNG

Cybersicherheit ist für Verwaltungen ein wichtiges Thema. Nicht nur ihre IT-Infrastrukturen an sich sind schützenswert, sondern auch und vor allem die durch die IT unterstützten Anwendungen in Staat und Gesellschaft. Neben der Verbesserung und Weiterentwicklung der klassischen IT-Sicherheitsmaßnahmen stellen die Vernetzung aller Beteiligten und deren koordiniertes Vorgehen wichtige Bausteine einer umfassenden Cybersicherheitsstrategie dar.

Verwaltungsrelevanz: ■■■■

Umsetzungsgeschwindigkeit: ■■■■ – ■■■■

Marktreife/Produktverfügbarkeit: ■■■■

SICHER SURFEN DANK DNSSEC?

Die Szene könnte aus einem Agententhriller stammen: Fünf Personen aus verschiedenen Teilen der Welt treffen sich an einem vereinbarten Ort. Jeder von ihnen hat einen Schlüssel dabei. Mit deren Hilfe öffnen sie gemeinsam einige Behälter und entnehmen den Inhalt. Kurz darauf machen sie sich an einem Computer zu schaffen. Mit den Worten: „Nun ist die Welt wieder sicher" zerstreuen sie sich wieder in alle Winde.

Rückblende: 1984 veröffentlichen vier Studenten die erste Implementierung für das sog. Domain Name System (DNS). Durch diese Technik sollten die bis dahin üblichen Listen auf Rechnern ersetzt werden, in denen die Rechnernamen in einem Netzwerk den technisch nutzbaren IP-Adressen zugeordnet wurden. Mit der wachsenden Zahl von Rechnern in den Netzen wurde die Pflege bzw. Verteilung dieser Listen aber immer schwieriger. Diese Listen mit dem Dateinamen HOSTS.TXT finden sich auch heutzutage noch auf modernen Rechnern. Sie werden aber lediglich für lokale Festlegungen genutzt. Das moderne „Telefonbuch" der Netzrechner ist das DNS. Vergleichbar einer Telefonauskunft können spezielle DNS-Server abgefragt werden, um zu einem Rechnernamen die zugehörige IP-Nummer zu ermitteln.

Als das DNS aufgebaut wurde, dienten entsprechende DNS-Server noch der technischen Vereinfachung, die die Administratoren entlasten sollte. In den Netzen vertraute man sich gegenseitig und so erfolgen die Abfrage des DNS-Servers, sog. DNS-Query, und die Erteilung einer Antwort, sog. DNS-Response, weitgehend ungeschützt. Das bedeutet einerseits, dass die Informationen unverschlüsselt übermittelt werden, und andererseits, dass es keine Möglichkeit gibt zu prüfen, wer eine Antwort geschickt hat. Das bietet die Möglichkeit für sog. „Man in the Middle"-Angriffe auf den DNS-Dienst. Dabei werden DNS-Abfragen abgefangen und mit einer falschen IP-Adresse beantwortet. Die kann für Werbe- oder kriminelle Zwecke aber auch zur Netzkontrolle durch Staaten genutzt werden. Auf diese Weise ist es z. B. möglich, durch die Umleitung auf eine nachgebaute Bankenseite Kontodaten der Nutzer von Onlinebanking auszuspähen.

Um die Authentizität der Absender von Nachrichten sicherzustellen, haben sich in der Vergangenheit Signaturverfahren mit asymmetrischen Schlüsseln etabliert. Dabei erzeugt der Absender mit Hilfe seines privaten und geheimen Schlüssels einen Code, der Informationen zu der eigentlichen Nachricht enthält. Diesen Code verschickt er zusammen mit der Nachricht. Der Empfänger kann mithilfe des sog. öffentlichen Schlüssels prüfen, ob der Code zu der Nachricht passt. Dadurch kann zum einen sichergestellt werden, dass die Nachricht nicht verfälscht wurde. Zum anderen kann der Empfänger sicher sein, dass die Nachricht vom erwarteten Absender kommt – solange dessen geheimer Schlüssel nicht kompromittiert wird.

Dieser Mechanismus soll mit den sog. Domain Name System Security Extensions, kurz mit DNSSEC, in das DNS eingebaut werden. Jeder DNS-Server, der mit DNSSEC arbeitet, signiert alle DNS-Informationen, die er versendet – die sog. DNS-Records – mit seinem geheimen Schlüssel. Die Empfänger dieser Nachrichten, die DNS-Clients, können mithilfe des öffentlichen Schlüssels sowohl die Authentizität als auch die Integrität der Nachricht überprüfen.

Immer, wenn von Verschlüsselung die Rede ist, kommt ein Parameter ins Spiel, der Einfluss auf die Sicherheit des Verfahrens hat – die sog. Schlüssellänge. Auch wenn die Schlüssellänge nicht direkt das Sicherheitsniveau des Kryptoverfahrens misst[1], kann man bei den asymmetrischen Vefahren zumindest sagen, dass mit wachsender Schlüssellänge die Sicherheit zunimmt. Allerdings hat die Verwendung längerer Schlüssel auch zur Folge, dass das Verschlüsseln, Signieren und Validieren aufwändiger wird. Für einen einzelnen Vorgang mag dieser Aufwand noch zu vernachlässigen sein. Wenn ein DNS-Server aber täglich mehrere zig-Millionen Abfragen beantworten muss, fällt dieser Aufwand ins Gewicht und es muss ggf. teure leistungsfähigere Hardware eingesetzt werden. Durch den Einsatz kürzerer Schlüssel könnte man den Rechenaufwand zwar verringern, jedoch müssten die DNS-Administratoren dann öfter die eigenen Schlüssel wechseln, um die Sicherheit zu gewährleisten. Dies würde also lediglich eine Verlagerung von Aufwand bedeuten.

Der Grundgedanke von DNSSEC klingt einfach und der Aufwand für die Einrichtung von DNSSEC auf einem einzelnen Knoten scheint auch überschaubar. Trotzdem hat es bisher über 15 Jahre gedauert, bis die ersten Schritte in Richtung eines operativen Betriebs gemacht werden konnten. Auch wenn die Notwendigkeit, das DNS abzusichern, früh erkannt wurde, braucht die Entwicklung eines internationalen Standards immer ihre Zeit – zumal dann, wenn viele Stellen tatsächlich von den Auswirkungen betroffen sind. In diesem Zusammenhang muss man sich die ungeheure Größe des Namensraums der Internetdomänen vor Augen führen und dabei bedenken, dass jeder Domänenname weltweit ein-

[1] s. dazu: http://de.wikipedia.org/wiki/Schl%C3%BCssell%C3%A4nge

deutig sein muss. Schon die erste Unterscheidungsebene, die sog. Top-Level-Domains, umfasste bis vor kurzem über 300 einzelne Domänen, davon allein rund 200 Ländernamen (z. B. .de für Deutschland, .at für Österreich oder .se für Schweden) sowie einige anderweitig festgelegte Namen (z. B. .com, .edu, .net oder .org). Mit der Öffnung des Namensraums für die Top-Level-Domains wurden Anfang 2012 fast 2.000 Bewerbungen um neue Einträge eingereicht. Auf der nächsten Ebene der Domänennamen – mit den sog. Second-Level-Domains – können dann z. B. Städte, Organisationen, Firmen oder auch Länder ihre Adressen einrichten. Die Dömäne .de ist dabei weltweit eine der größten und verfügte im Frühjahr 2012 bereits über rund 15 Mio. Einträge für Second-Level-Domänen.

Für DNSSEC hat die zwar flache, aber sehr breite Hierarchie der Domänen Einfluss auf die Dauer der Einführung. Um die durchgehende Authentizität aller DNS-Server gewährleisten zu können, müssen die verschiedenen Domänen über alle Domänenebenen von oben nach unten signiert werden. Die 13 DNS-Server der sog. Root-Domäne – sozusagen der Punkt von „.de", „.com" usw. – sind seit Mai 2010 mit den notwendigen Zertifikaten versehen und mit DNSSEC ausgestattet. Als „oberste Instanz" in der Hierarchie der Domänennamen spielt die Root-Domäne eine besondere Rolle. Dies gilt umso mehr, als sie nicht der organisatorischen und rechtlichen Kontrolle eines einzelnen Landes unterstellt werden soll. Daher hat man sich bei der Einführung von DNSSEC darauf verständigt, die Berechtigung und Befähigung zur Erzeugung neuer Schlüssel für diese kritische Domäne in die Hände von international anerkannten Vertrauenspersonen – sog. Trusted Community Representatives – zu legen. Drei Teams à sieben Mitgliedern wurden eingesetzt, von denen jeweils fünf Personen wie in der eingangs geschilderten Szene gleichzeitig anwesend sein müssen, um mit ihren Zugangsberechtigungen neue Schlüssel zu erzeugen.

Im Juli 2010 wurde die Domäne .org signiert und seit Mitte 2011 sind die 16 Server, die für die Domäne .de den DNS-Dienst übernehmen, ebenfalls auf DNSSEC umgestellt. Damit ist .de eine von rund 100 Top-Level-Domains, die bis August 2012 signiert waren.

Neben der schieren Masse der DNS-Server, die auf DNSSEC umgestellt werden müssen, hat die Einführung der Sicherheitsfunktionen auch noch mit weiteren Herausforderungen zu kämpfen. So konnte der Einsatz von DNSSEC mit dem weit verbreiteten Nameserver BIND zu Speicherproblemen führen. Neben solchen technischen Problemen, die mit einem Update der Software behoben werden können, gibt es aber auch neue Grundsatzdiskussionen im Zusammenhang mit DNSSEC: Die Verwendung signierter Domäneninformationen verhindert nicht nur das böswillige Fälschen von Namensauflösungen, sondern auch die „kommerzielle" Nutzung vom DNS-Umleitungen durch Provider oder die staatlich verordnete Umleitung im Zusammenhang mit Straftaten. Manche Internetprovider reagieren auf falsch eingegebene Webadressen, indem sie die Benutzer auf ihre Suchseiten umleiten, anstatt eine einfache Fehlermeldung auszugeben. Dieser Mechanismus kann jedoch bei anderen Internetanwendungen neben der reinen Browsernutzung zu Problemen führen, da sie nicht die Fehlermeldung erhalten und somit annehmen, die vermeintlich korrekte Zielseite erreicht zu haben. Auch DNS-Sperren oder –Umleitungen, die z. B. den Diebstahl von geistigem Eigentum verhindern sollen, lassen sich mit DNSSEC nicht realisieren, da hier die Veränderung einer Zieladresse leicht erkannt werden kann.

Selbst wenn die technischen und politischen Hürden der Einführung überwunden werden und DNSSEC weit verbreitet ist, bedeutet das nicht, dass das Internet insgesamt dann sicher ist. Durch DNSSEC sind die Informationen aus dem DNS nachprüfbar. Doch verläuft die Kommunikation zwischen DNS-Server und –Client weiterhin unverschlüsselt. Dadurch kann sie einerseits mitgelesen und andererseits manipuliert werden. So verwundert es nicht, dass zu DNSSEC bereits Alternativen – z. B. DNS-Curve – oder Ergänzungen – z. B. DNS-Crypt – entwickelt werden, die die Kommunikation zusätzlich absichern sollen. Bis DNSSEC wirklich flächendeckend nutzbar ist, wird es noch einige Jahre dauern. Welchen Einfluss bis dahin Ergänzungen und Alternativen auf die weitere Einführung haben, dürfte für die Sicherheit im Internet eine wichtige Frage sein.

BEWERTUNG

Öffentliche Verwaltungen sind auch heute noch nur sehr bedingt Anbieter von kritischen Online-Diensten für Nutzer. Während im kommunalen Bereich noch vergleichsweise viele E-Government-Dienste und verwaltungsnahe, evtl. kostenpflichtige, Leistungen für Kunden erbracht werden, sind derlei Anwendungen bei Bund und Ländern nur vereinzelt vorhanden. Von daher besteht für Verwaltungen oft kein akuter Handlungsdruck aufgrund von Kundennachfrage zur Einführung von DNSSEC. Auf der anderen Seite ist es auch im Interesse der Verwaltungen – nicht zuletzt selber als Nutzer – die Sicherheit im Internet zu verbessern. Von daher empfiehlt es sich, mittelfristig auch alle Verwaltungsdomänen durch DNSSEC abzusichern.

Verwaltungsrelevanz: ■■■□ / ■■□□

Umsetzungsgeschwindigkeit: ■□□□

Marktreife/Produktverfügbarkeit: ■■■■

DO NOT TRACK!

Der Werbemarkt ist heiß umkämpft. Klassische Zeitschriften finanzieren sich zumeist nur noch über die verkauften Anzeigen, die darin geschaltet werden. Der Inhalt ist nur noch wichtig, um die Zielgruppe der Werbung zu definieren. Für Werbung im Internet wird nach einzelnen Berichten 2012 in den USA erstmals mehr Geld ausgegeben als für gedruckte Werbung. Dabei ist die Rede von 39,5 Mrd. Dollar für Online-Anzeigen gegenüber 33,8 Mrd. Dollar für den Print-Bereich. Auch wenn diese Zahlen noch nicht objektiv nachprüfbar sind, vermitteln sie zumindest einen Eindruck von den Dimensionen, in denen sich der Werbemarkt bewegt. In Deutschland sind die entsprechenden Budgets zwar deutlich kleiner. Aber auch hier spielt die Werbung eine wichtige Rolle in den Geschäftsmodellen von Online-Angeboten.

Einer der Erfolgsfaktoren von Werbung ist es, die richtigen Personen anzusprechen. Und da ist es natürlich verlockend, Internetnutzer anhand ihres Surfverhaltens zu analysieren und entsprechende Anzeigen einzublenden.

Die Analyse des Surfverhaltens erfolgt in der Regel durch sog. „User-Tracking". Dieser Begriff wird auch im Zusammenhang mit Usability-Tests für Software verwendet. Im Unterschied zu diesen Tests werden hier aber nicht die einzelnen Benutzeraktionen beobachtet, sondern die besuchten Webseiten protokolliert. Aus diesen lassen sich – bis zu einem gewissen Grad – die Interessen der Nutzer ableiten. Und so darf es dann nicht verwundern, wenn man nach dem Besuch von Webseiten zu einem Hobby plötzlich Werbung für einschlägige Literatur eingeblendet bekommt.

Weit verbreitet ist das User-Tracking durch sog. Tracking-Cookies. Cookies sind kleine Dateien, die durch Webseiten auf dem Rechner des Benutzers gespeichert werden. Zumeist handelt es sich um reine Text-Dateien; Cookies können aber auch spezifische Datenformate haben (z. B. sog. Flash-Cookies). Die Text-Cookies werden entweder im sog. Header einer HTTP-Anfrage (s.u.) transportiert und daher auch als HTTP-Cookies bezeichnet, oder sie werden durch Skripte oder andere ausführbare Seitenbestandteile lokal auf dem Rechner des Nutzers generiert. Ursprünglich waren Cookies entworfen worden, um Nutzereinstellungen in Webanwendungen zu simulieren, indem die Parameter in den separaten Dateien gespeichert werden.

Das Aufzeichnen des Surfverhaltens von Nutzern wird häufig als Datenschutzproblem gesehen. Kann man noch davon ausgehen, dass ein Nutzer, der eine bestimmte Webseite aufsucht, damit einverstanden ist, dass der entsprechende Server davon Kenntnis erhält, wird es zunehmend als kritisch empfunden, wenn derartige Informationen an Dritte – z. B. Werbefirmen – gelangen.

Um die Analyse des Surfverhaltens – insbesondere durch Dritte – einzuschränken, wurde eine Initiative gestartet, die die „Do not track"-Technik (DNT) zum Webstandard machen möchte. DNT verwendet ebenfalls Eigenschaften des HTTP-Headers, um Servern mitzuteilen, dass der Nutzer kein User-Tracking wünscht. Die Nachrichten des Hypertext-Transfer-Protocols (HTTP) bestehen aus einem Kopf (engl. „header") und der eigentlichen Nachricht im „Body". Im „Header" können einzelne Werte in verschiedenen Datenfeldern untergebracht werden. DNT ist ein solches HTTP-Header-Feld, das mit dem Wert „1" das Trackingverbot übermittelt. Der Wert „0" gibt an, dass das Tracking erlaubt ist. Welcher Wert übermittelt wird, soll der Nutzer in seinem Browser einstellen. Die Standard-Einstellung eines Browsers soll zunächst sein, dass das Feld nicht übertragen wird – also kein explizites Tracking-Verbot voreingestellt ist. Entgegen dieser Vereinbarung will Microsoft in seinem Internetexplorer 10 jedoch das Tracking-Verbot, also den Wert „1", als Standard setzen.

Noch ist DNT kein Webstandard. Das World Wide Web Consortium, kurz W3C, hat jedoch mit der „Tracking Protection Working Group" eine Arbeitsgruppe eingerichtet, die daran arbeitet. Anfang 2013 sollen die wesentlichen Punkte der künftigen „Empfehlung" – wie die W3C-Standards offiziell heißen – feststehen, sodass dann ein sog. Empfehlungskandidat vorliegen soll. Die endgültige Fassung ist für April 2013 vorgesehen.

Die relativ einfache Funktionsweise des DNT-Feldes ist zugleich auch eine Schwäche dieses Versuchs, die Privatsphäre von Surfern besser zu schützen. Die Übermittlung des Tracking-Verbots nützt nur dann etwas, wenn ein Server, der diese Nachricht erhält, deren Inhalt auch berücksichtigt. Dies geschieht bisher auf freiwilliger Basis. Der Ansatz ist daher ähnlich der „Steuerung" von automatischen Suchmechanismen – sog. Webcrawlern – durch Direktiven in der Serverdatei robots.txt. Auch hier kann nicht erzwungen werden, dass sich die Suchroboter daran halten, welche Verzeichnisse auf dem Server für sie verboten sind.

Die EU-Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) regelt Möglichkeiten und Einschränkungen der Übermittlung von Informationen. Die Interpretation in Bezug auf die Verwendung von Cookies ist in den zugehörigen Gründen, Nr. (25), dargelegt. Danach soll es Nutzern möglich sein, die Speicherung von Cookies auf einem Endgerät zu verbieten. Zudem wird auch gefordert, dass die Einholung der Zustimmung zur Nutzung von Cookies „so benutzerfreundlich wie möglich" sein soll.

Eine Gesetzesinitiative in den USA geht in Sachen Tracking-Verbot sogar noch weiter: Dort könnte beschlossen werden, dass „Do not track" eine rechtlich bindende Willensäußerung des Nutzers darstellt. Es ist nicht verwunderlich,

dass Firmen, die wesentlich von Nutzerprofilen und auf den Nutzer abgestimmter Werbung profitieren, vor den Folgen einer solchen Regelung warnen. Sie argumentieren, dass die schwindenden Werbeeinnahmen dazu führen würden, dass sich das Internetangebot – insbesondere an freien Seiten – wesentlich reduzieren könnte. Die Nutzer würden sich durch die Aktivierung von DNT also nur selbst schaden.

Die Brisanz von Mechanismen und Regelungen zum User-Tracking wird deutlich, wenn man sich mögliche Strafen für den missbräuchlichen Einsatz von Cookies vor Augen führt. So musste ein großer Dienstanbieter eine Vergleichsstrafe von 18,2 Millionen Euro bezahlen, da er mit einem Trick die Privatsphäreeinstellungen eines bestimmten Browsers umgangen hatte und deren ungeachtet Cookies auf den entsprechenden Rechnern installierte. Rechtsexperten hatten ausgerechnet, dass dem Konzern eine Strafe in Höhe von 800 Milliarden Dollar drohe. Gegen ein Soziales Netzwerk wurde wegen der Verletzung der Privatsphäre geklagt. Der nominelle Schadenswert beläuft sich auf 15 Milliarden Dollar. Dies entspricht ungefähr dem Wert des Unternehmens bei seinem Börsengang.

BEWERTUNG

Das Internet wird auch in den öffentlichen Verwaltungen intensiv genutzt. Webbrowser sind an IT-Arbeitsplätzen und auf mobilen Endgeräten in der Regel als Standardkomponenten vorhanden. Damit sind auch hier die Mitarbeiterinnen und Mitarbeiter vom Einsatz von Tracking-Cookies betroffen. Die Einblendung spezifischer Werbung mag noch das kleinste Problem sein. User-Tracking kann aber nicht nur zu Werbezwecken, sondern auch zu weiterführenden Analysen des Nutzerverhaltens eingesetzt werden. Die möglichst verlässliche Unterbindung der Installation von Tracking-Cookies scheint hier also wünschenswert. Dies gilt insbesondere dann, wenn Geräte sowohl dienstlich als auch privat genutzt werden können (s. „BYOD – Bring Your Own Device", HZD-Trendbericht 2012). Der Einsatz eines modernen Browsers ist für die Einrichtung von DNT jedoch Voraussetzung.

Auch als Anbieter von umfangreichen Webdiensten sind öffentliche Verwaltungen gehalten, die Handhabung von Nutzerprofilen auf den Einsatz von Cookies zu prüfen und ggf. DNT-kompatibel zu gestalten.

Verwaltungsrelevanz: ■■■□

Umsetzungsgeschwindigkeit: ■■■■

Marktreife/Produktverfügbarkeit: ■■■□

05_ TECHNIK

DER STOFF, AUS DEM DIE TRÄUME SIND – NEUE NETZE

Die Welt der Computer wird immer bunter, vielfältiger, mobiler. Smarte Geräte tragen die „Informationstechnik" in nahezu alle Lebensbereiche und „höher, schneller, weiter" scheint auch dabei das Leitmotto zu sein. Mit mehr Bandbreite, mehr Funkzellen, mehr Speicher und mehr Anwendungen werden beruflicher und privater Alltag zunehmend digitalisiert und miteinander verwoben. Doch ein „immer mehr" von den vorhandenen Techniken reicht nicht aus, um alle neuen Anforderungen – oder Wünsche –, die ein solches digitalisiertes Leben mit sich bringt, zu befriedigen. So hat die Verknüpfung von verschiedenen, zuvor mehr oder weniger stark getrennten Lebensbereichen die Entwicklung von Cloud-Technologien befördert. Der Wunsch oder die Notwendigkeit jederzeit und überall auf „seine" Daten und Anwendungen zugreifen zu können, lässt sich mit etablierten Techniken wie Client/Server-Modellen und Replikation von Daten nur noch bedingt befriedigen. Also entstehen neue Modelle der Daten- und Anwendungsbereitstellung. Die präsentieren sich auf Smartphones und Tabletts in neuem Gewand und Dank immer schneller werdender Netze fällt die Abhängigkeit von zentralen – oder besser „allgegenwärtigen" – Infrastrukturen fast nur noch auf, wenn man in ein Funkloch gerät.

Man könnte also meinen, dass sich die Technik im Hintergrund unaufhaltsam weiterentwickelt, während wir uns am „Frontend" über Apps, Internet-TV oder schnelle und schicke Businessanwendungen freuen. Doch das „höher, schneller, weiter" im Backend hat – wie überall – seine Grenzen. Diese wurde z. B. durch die Verknappung von IP-Adressen deutlich. Durch die Art und Weise, wie die Geräteadressen in Version 4 des Internetprotokolls gebildet werden, lassen sich nicht überall beliebig viele Adressen vergeben. So wird mancherorts der Vorrat an Adressen für neue Computer, Smartphones oder andere Komponenten langsam aber sicher knapp – von den Adressen für ein Internet der Dinge mit vernetzten Kühlschränken und anderen Alltagsgegenständen ganz zu schweigen. Die nächste Generation des Internetprotokolls, kurz „IPv6" genannt, scheint dieses Problem zwar durch einen viel größeren Adressraum zu lösen. Doch verschärft dies die Frage, wie das Routing – also die Navigation von Datenpaketen zu den IP-Adressen – möglichst schnell und einfach realisiert werden kann, denn im mobilen Zeitalter kann sich jede IP-Adresse nahezu überall auf der Welt befinden, wenn sie an ein mobiles Gerät gebunden ist.

Auch Virtualisierung, Cloud-Technik oder die wachsende Zahl an hochauflösenden Videos, die in der Datenwelt unterwegs sind, bringen traditionelle Netze an die Grenzen ihrer Leistungsfähigkeit. Galt vor Kurzem noch 10 Gigabit-Ethernet, kurz 10GbE, als vollkommen ausreichend, sind nun 40GbE und 100GbE mit Übertragungsraten von 40 resp. 100 Gigabit pro Sekunde der Stand der Entwicklung. Doch diese Geschwindigkeit hat ihren Preis: Zum einen sind – wörtlich genommen – Geräte, die die neuen Verbindungen unterstützen, noch relativ teuer. Zum anderen hat

die hohe Geschwindigkeit auch funktionale Auswirkungen: Um z. B. eine Echtzeitanalyse von Daten in einem 100GbE bei Volllast durchführen zu können, müssten pro Minute 750 MByte – etwa eine CD-Rom – verarbeitet werden. So wird etwa Intrusion-Detection, die möglichst zeitnah erfolgen muss, zu einer technischen und finanziellen Herausforderung.

Daneben sehen Experten eine weitere Herausforderung in den schnellen Netztechniken entstehen: den Energiebedarf der Netzkomponenten. In einem Router wird Energie nicht nur für die Schaltvorgänge benötigt. Diese ist zwar mit ca. zehn Nanojoule pro Bit relativ gering, würde aber bei 100 GBit/s auch schon ausreichen, um einen Liter Wasser in knapp 10 Minuten zu Kochen zu bringen. Bedenkt man, dass die aufgenommene Leistung eines Routers nur zu einem Teil in den Schaltvorgang fließt und ein wesentlicher Teil als Wärme wieder abgeführt werden muss, wird deutlich, dass in der Wärmeentwicklung eine echte Herausforderung besteht. Spezialisten halten 10 TBit/s für die Grenze des Machbaren.

Und auch die etablierten Netzprotokolle gelangen an ihre Grenzen. Der größte Teil der Datennetze verwendet heute das Internetprotokoll und somit erfolgt die Datenübertragung in Datenpaketen. Die Idee der Paketvermittlung war dabei, dass sich die Daten so ihren Weg selber durch das Netz bahnen – bzw. entsprechend der tatsächlich zur Verfügung stehenden Transportwege durch das Netzwerk geführt („geroutet") werden. Im Gegensatz zu der seinerzeit üblichen Technik in Telefonnetzen – der sog. Leitungsvermittlung – muss damit nicht eine separate Leitung zwischen Sender und Empfänger „geschaltet" werden, über die dann die komplette Übertragung abgewickelt wird. Bei der Paketvermittlung können die Datenfragmente grundsätzlich auch unterschiedliche Wege nehmen. Sie müssen beim Empfänger lediglich wieder in der richtigen Reihenfolge zusammengesetzt werden. Was so einfach klingt, wird bei der Übertragung eines hochauflösenden HD-Videos zur Herausforderung, wenn – bildlich gesprochen – die Datenberge vom Ende des Films vor denen vom Anfang geliefert werden und die Auflösung eines spannende Krimis ausbleibt, weil Datenpakete wegen eines überfüllten Puffers verworfen wurden.

Doch es sind nicht nur Videos und Anwendungsdaten, die in immer größerem Umfang transportiert werden müssen. In virtualisierten Rechenzentren und noch mehr in einer Cloud müssen bei Bedarf ganze Rechnerumgebungen über die Netze geschoben werden. Solange sich die Einrichtung und der Betrieb eines virtuellen Servers innerhalb eines Geräteschrankes abspielt, stellt das Netzwerk dabei kaum ein Hemmnis dar. Wenn aber virtuelle Arbeitsumgebungen etwa aus Gründen der Lastverteilung zwischen verschiedenen Rechenzentren „verschoben" werden müssen, spielen Bandbreiten und Netzwerktopologie eine wesentliche Rolle. In den etablierten Datennetzen werden die Datenpakete auf ihrem Weg vom Sender – z. B. einem Server oder einem Arbeitsplatzrechner – zum Empfänger über verästelte Netzabschnitte geleitet. Zunächst werden zu einem zentralen

Router, sog. Core-Router, dirigiert, von wo aus sie – wiederum über verschiedene Netzstrecken – an den Adressaten gelangen. Die einzelnen Strecken ergeben idealerweise einen Baum, das heißt einen zusammenhängenden und schleifenfreien Graphen. Auch wenn diese Struktur relativ überschaubar ist, bedeutet sie für die Datenübertragung evtl. lange Wege mit vielen Zwischenstationen.

Eine Lösung für die daraus entstehenden Probleme besteht darin, „Abkürzungen" zwischen vielen Punkten im Netz einzubauen. In einer schematischen Darstellung erinnert dann das Bild, in dem jeder Datenlieferant mit jedem Empfänger verbunden ist, an ein Stück gewobenen Stoff. Daher spricht man hier auch von Switched Fabric – oder kurz nur Fabric. Doch wird damit die Steuerung der Datenflüsse einfacher? Bisher findet die Steuerung von Datenpaketen zumeist auf Ebene 3 (engl. „Layer 3", kurz „L3") – der sog. Vermittlungsschicht – des OSI-Schichtenmodells statt. Dieses Modell beschreibt, wie Informationen in Netzen transportiert werden – von der logischen Sicht der Anwendung (Ebene 7, L7) über die Kapselung in verschiedenen „Paketgrößen" bis hin zur physikalischen Sicht (Ebene 1, L1), in der beschrieben wird, wie die Bits tatsächlich durch elektrische oder optische Signale über Leitungen transportiert werden. Im Zuge der Beschleunigung von Netzwerken durch die bessere Nutzung und Auslastung der zur Verfügung stehenden Verbindungen wir die Steuerung des Datenflusses auf Ebene 2 (L2) – die sog. Sicherungsschicht – verlagert. Hier kann mithilfe neuer Protokolle das Routing anhand von Ressourceninformationen optimiert werden, ohne wie beim L3-Routing den Weg anhand der IP-Nummer im Datenpaket zu bahnen. Ein Beispiel für ein solche Layer 2 Multipath-Protokoll (L2PM) ist TRILL (kurz für „Transparent Interconnect of Lots of Links").

Die neuen Protokolle sind noch längst nicht alle standardisiert und Begriffe wie Fabric werden noch uneinheitlich genutzt. So kommt es derzeit noch sehr auf die Sichtweise – und das Leistungsspektrum – der Provider an, was sich in einem Fabric-Produkt verbirgt. Eigenschaften, die für solche Produkte gefordert werden, umfassen u. a.

- Sicherheit beim Transport der Daten,
- geringe Laufzeitverzögerung (engl. „Latency") und Laufzeitvarianz (engl. „Jitter"),
- any-to-any-Verbindungen,
- Skalierbarkeit und Elastizität sowie
- Effizienz und Intelligenz bei der Optimierung der Übertragung.

Da es keine scharfe Definition für Fabric – und somit für deren Einsatzbereiche – gibt, werden folgende Indikatoren genannt, bei deren Auftreten der Einsatz der neuen Techniken geprüft werden sollte:

- Performance-Engpässe im Netzwerk,
- Engpässe bei Strom- und Kühlungsversorgung oder beim Platz im Rechenzentrum,
- Migration von virtuellen Maschinen über einzelne Geräteschränke hinweg,
- Neugestaltung von Netzwerken oder
- Konsolidierung von Rechenzentren.

Das Bild, wie neue Netze – insbesondere im Rechenzentrum – aussehen, beginnt sich zu verändern. Die wachsenden Anforderungen erzwingen Lösungen, die nicht allein in der Verbesserung der etablierten Techniken bestehen, sondern zu grundlegend neuen Strukturen und Techniken führen. Da sich die Grundlagen dieser „neuen Netze" aber noch entwickeln, die entsprechenden Techniken ihre optimalen Anwendungsbereiche finden müssen und nicht kurzfristig flächendeckend vorhandene Netze gegen neue Strukturen ausgetauscht werden können, werden viele der neuen Ansätze – sofern sie sich durchsetzen – noch eine ganze Weile neben den traditionellen Netzen existieren müssen.

BEWERTUNG

Datennetze bilden das informationstechnische Rückgrat der öffentlichen Verwaltungen. Auch wenn viele Vorgänge noch immer nicht vollständig auf Papier verzichten können, ist auch eine gut vernetzte IT für deren Effizienz unerlässlich. Die meisten Verwaltungen tragen den daraus resultierenden Anforderungen mit ihren bestehenden Netzen Rechnung. Doch auch für die IT im öffentlichen Bereich gewinnen wachsende Datenmengen, Virtualisierung und Cloud-Techniken massiv an Bedeutung. Videos sind hier zwar keine Standardinhalte. Sie haben auf der anderen Seite aber auch ihren Status als verzichtbares Medium verloren – z. B. zur Dokumentation von Ereignissen oder als Material in der Fortbildung. Die öffentlichen IT-Dienstleister werden prüfen müssen, ob die neuen Netztechniken auch den gestiegenen Anforderungen an die IT-Sicherheit genügen („Kritische Infrastrukturen"). Für die Nutzer ist die eingesetzte Netztechnik im besten Fall nicht wahrnehmbar. Für sie zählt der reibungslose Betrieb von Fachverfahren, Anwendungen und Diensten. Und diese Erwartung zwingt zu einer kontinuierlichen Weiterentwicklung der Netze.

Verwaltungsrelevanz: 

Umsetzungsgeschwindigkeit: 

Marktreife/Produktverfügbarkeit: 

MIT SSD-VERSCHLÜSSELUNG ZUM SUPER-SICHEREN DEVICE?

Daten und Programme auf Computern sollen in der Regel schnell verfügbar und sicher gespeichert sein. Die Geschwindigkeit des Datentransfers ist bei Festplatten zwar schon um einiges höher als bei Bandlaufwerken, für manche Zwecke werden aber noch schnellere Permanentspeicher benötigt. Das hat zur Entwicklung von sog. Solid State Disks, kurz SSDs, geführt (vgl. HZD-Trendbericht 2010). In SSDs finden sich keine beweglichen Teile: Die Speicherung der Daten erfolgt nicht auf rotierenden Platten sondern in Speicherbausteinen – sog. NAND-Flash-Speichern – und der empfindliche Schreib-/Lesekopf kann somit auch entfallen. Das macht die SSDs nicht nur sehr schnell und robust sondern auch leise. Damit wären SSDs eigentlich die idealen Speicher. Doch auch sie haben eine bauartbedingte Schwachstelle. Ihre Haltbarkeit ist – je nach eingesetzter Technik – auf 3.000 bis 100.000 Schreib- oder Löschvorgänge begrenzt. Das mag für den normalen Gebrauch eines solchen Speichers ausreichend sein. Für datenintensive Anwendungen kann es aber ein Betriebsrisiko darstellen. Und für die Sicherung von SSDs mittels Verschlüsselung hat das ebenfalls Konsequenzen.

Wer die in seinem Computer gespeicherten Daten verschlüsseln möchte, kann dies auf verschiedenen Ebenen der Dateiablage tun: einzelne Dateien und Ordner lassen sich durch entsprechende Programme verschlüsseln. Dies ist auf der einen Seite recht flexibel, da man für verschiedene Objekte auch unterschiedliche Schlüssel verwenden kann. Es bedeutet aber auch, dass man jedes Mal beim Gebrauch der Daten für Entschlüsselung und Verschlüsselung sorgen muss.

Komfortabler ist es, wenn ganze Laufwerke oder zumindest einzelne Partitionen verschlüsselt werden können und das Codierungsverfahren zentral gesteuert wird. Diese sog. Full Disk Encryption (FDE) kann mittels einer Software erfolgen oder der Controller des Gerätes übernimmt diese Aufgabe. Bei der Hardware-basierten Verschlüsselung spricht man dann auch von „selbst verschlüsselnden Geräten" (engl. Self-Encrypting Device, kurz SED).

Überlässt man die Ver- und Entschlüsselung ohne jedes Eingreifen des Nutzers ausschließlich der Technik, ist das zwar in der Handhabung sehr bequem. Es stellt sich aber dann die Frage nach dem Mehrwert der Verschlüsselung, denn jeder, der das Gerät in den Betriebszustand versetzen kann, erhält dann auch Zugriff auf die entschlüsselten Daten. Daher wird die Hardwarelösung häufig durch einem Passwortschutz im BIOS ergänzt. Beim Einschalten des Gerätes wird dann zunächst dieses Passwort abgefragt, bevor auf den Inhalt zugegriffen werden kann.

Für die Verschlüsselung der Daten werden in der Regel als sicher geltende Verfahren mit ausreichender Schlüssellänge eingesetzt. Doch hier lohnt es sich, genau hinzuschauen: In einem Fall wurde zwar ein starkes Verschlüsselungsverfahren verwendet, um den Datenschlüssel zu verbergen. Die eigentliche Datenverschlüsselung erfolgte aber mit einem sehr schwachen Algorithmus (XOR-Verschlüsselung mit festem, relativ kurzem Schlüssel). Dadurch ließ sich der Platteninhalt auch ohne Kenntnis des gut geschützten Schlüssels vergleichsweise einfach decodieren. In einem anderen Fall stimmte die Herstellerangabe der verwendeten Schlüssellänge nicht: Anstelle des angegebenen AES-Verfahrens mit einem 256 Bit-Schlüssel wurde AES lediglich mit 128 Bit Schlüssellänge eingesetzt.

Das bis hier Gesagte über Verschlüsselungstechniken gilt sowohl für Festplatten wie auch für SSDs. Bei den Solid State Drives sind aber noch einige Besonderheiten zu beachten, die sich aus der Technik ergeben: Wie weiter oben gesagt, ist die Lebensdauer der Speicherzellen in einer SSD begrenzt. Daher werden in SSDs in der Regel Algorithmen eingesetzt, die ein gleichmäßiges Beschreiben und somit die gleichmäßige „Abnutzung" der Speicherzellen gewährleisten sollen – sog. Wear Leveling-Verfahren.

Damit hat das Wear Leveling Einfluss auf die Sicherheit von SSDs: Das Löschen von Daten erfolgt häufig durch eine Markierung der zugehörigen Speicherzellen. Der Inhalt wird dann dabei nicht verändert. Auch vermeintlich defekte Zellen, die nicht mehr beschrieben werden können, können noch ihren alten Inhalt haben und werden lediglich für die weitere Benutzung gesperrt. Damit der nutzbare Speicherplatz des Gerätes nicht zu schnell abnimmt, haben SSDs einen Bereich für Reservesektoren – bis zu zehn Prozent der Speicherkapazität. Die Nutzung dieses Bereichs wird durch die SSD-internen Verfahren gesteuert. Somit ist es nicht möglich, die entsprechenden Speicherzellen mit Standardsoftware gezielt zu löschen. Durch mehrfaches Überschreiben der gesamten nutzbaren SSD steigt auch die Wahrscheinlichkeit, dass auch die Reservesektoren überschrieben werden. Aber dies ist nicht wirklich sicher und geht zu Lasten der Lebensdauer des gesamten Speichers.
Das Löschen von Daten, die im Klartext vorliegen oder die mit einem kompromittierten Schlüssel codiert sind, ist bei

SSDs also nicht so einfach möglich. Das birgt einerseits ein Sicherheitsrisiko, erfreut aber andererseits diejenigen, die mit der Rettung von Daten auf defekten Geräten befasst sind.

Das Wear Leveling hat auch zur Folge, dass bei der nachträglichen Verschlüsselung einzelner Dateien, die auf der SSD gespeichert sind, nicht unbedingt der Klartext überschrieben wird. Stattdessen wird das codierte Ergebnis in andere Sektoren geschrieben und die unverschlüsselten Daten bleiben zunächst im Speicher, um das echte Löschen zu sparen. Dort sind sie nicht mehr über den normalen Dateizugriff lesbar. Sie können aber mit „forensischen" Methoden, die gezielt auf einzelne Speicherbereiche zugreifen können, evtl. wieder rekonstruiert werden. Daneben gibt es Verschlüsselungsanwendungen, die nicht nur die eigentlichen Daten verschlüsseln, sondern zusätzlich auch noch freien Speicherplatz mit Zufallszahlen auffüllen, um den „Füllstand" des Gerätes zu verbergen. Dies führt zu einer zusätzlichen Abnutzung der Speicherzellen.

Für die Rettung von Daten stellt die sichere Verschlüsselung eine besondere Hürde dar: Wenn das Passwort für die Entschlüsselung verlorenging oder absichtlich geändert wurde, kann dieses eventuell rekonstruiert werden. Ansonsten findet auch der Retter auf dem Gerät nur unverständlichen Zahlensalat. Der bleibt auch zurück, wenn der Schlüssel zur Codierung der Daten verändert wird – ohne dass die damit Daten umgeschlüsselt werden. Dies machen sich Sicherungsmechanismen in selbstverschlüsselnden Geräten zunutze. Wenn die Sicherheit des Gerätes bedroht ist, wird durch eine Firmwarefunktion der Schlüssel geändert. Als Auslöser dieser „Wipe"-Funktion kann z. B. ein explizites Kommando, der Wegfall der Versorgungsspannung oder der Einbau des Gerätes in einen anderen Rechner festgelegt werden. Allerdings sind dann die Daten endgültig verloren und das Gerät ist wertlos – auch für den Eigentümer.

Die beschriebenen Szenarien machen deutlich, dass die praktische Handhabung, die Sicherheit und die Wiederherstellung von Daten im Fehlerfall in einem Spannungsverhältnis stehen: Die Sicherheit der Daten sollte nicht – wie im Falle der dateiweisen Verschlüsselung – zu unangemessenem Aufwand führen. Das legt die Nutzung von Full Disk Encryption nahe, die aber nur wirkt, wenn sie nicht aus Versehen deaktiviert werden kann. Auf der anderen Seite können Daten ggf. auch verloren sein, wenn Schlüssel verlorengehen. Von daher entbinden sichere Verschlüsselungsverfahren auf schnellen Geräten nicht davon, ein Backup der Daten anzulegen – und zwar in einer Art und Weise, dass die Daten ggf. von berechtigten Personen auch verlässlich wiederhergestellt werden können.

Solid State Drives, die vor rund sechs Jahren auf den Markt kamen, beginnen in vielen Bereichen, die Festplatten zu verdrängen. Noch sind sie allerdings bezogen auf das Speichervolumen teurer als die klassischen Massenspeicher. Auch gilt ihre Firmware noch als anfällig, so dass sie längst nicht deren Betriebssicherheit erreicht haben – zumindest in normalen Arbeitsumgebungen. Ihre mechanische Robustheit legt dennoch evtl. den Einsatz für das mobile Arbeiten nahe. In jedem Fall kann die automatische Verschlüsselung von SSDs nur ein Baustein der Datensicherheit sein.

BEWERTUNG

Die Absicherung von Daten – insbesondere auf mobilen Geräten – ist in öffentlichen Verwaltungen ein wichtiges Thema und lange geübte Praxis. Hier geht aber die angemessene Sicherheit über den Komfort schneller Geräte. Daher ist vor der Verwendung selbstsichernder SSDs im Einzelfall zu prüfen, ob die tatsächlich implementierten Sicherheitsfunktionen für den geplanten Einsatz ausreichend sind. An normalen Büroarbeitsplätzen können die schnellen Geräte ein guter Kompromiss aus Komfort und zusätzlicher Sicherheit für lokale Daten sein, solange verlässliche Backup-Maßnahmen etabliert sind. Die genannten Aspekte der Betriebssicherheit und der Kosten legen es allerdings nahe, den massenweisen Einsatz zunächst noch zurückzustellen.

Verwaltungsrelevanz: ■■□□

Umsetzungsgeschwindigkeit: ■■■■

Marktreife/Produktverfügbarkeit: ■■■■-■■■□

... ZUR NOT AUCH TELEFONIEREN – VOICE OVER LTE

Wer das Wort „Mobilfunk" hört, denkt wohl zunächst an das Telefonieren mit dem Handy. Die Geräte sind – heute als gut ausgestattete Smartphones – zu Alltagsgegenständen geworden und die neuste Technik im Hintergrund gehört inzwischen zur sog. vierten Generation. Der Mobilfunkstandard LTE (kurz für „Long Term Evolution") breitet sich langsam aus und Geräte, die die schnelle Technik unterstützen, erscheinen am Markt. Den Hauptvorteil – Geschwindigkeit – spielt LTE in Verbindung mit Anwendungen auf mobilen Endgeräten oder als Ersatz für schnelle Festverbindungen in unterversorgten Gebieten aus. Doch wer meint, dass man mit LTE auch telefonieren kann, sieht sich – zunächst einmal – getäuscht. Natürlich kann man mit LTE-fähigen Handys auch telefonieren. Doch dabei kommt LTE nur bedingt zum Einsatz. Das liegt daran, dass LTE eine sog. „All-IP"-Technologie ist, bei der alle Informationen in einzelnen

Datenpaketen per Internet-Protokoll (IP) übertragen werden. Die bisherigen Mobilfunktechniken waren dagegen alle leitungsvermittelt, d. h. zwischen Sender und Empfänger wird zunächst eine Verbindung geschaltet, über die alle Daten übertragen werden. (Zur Thematik IP vs. Leitungsvermittlung s. S. 34, „Der Stoff, aus dem die Träume sind – neue Netze").

Um auf LTE-Handys das Telefonieren zu ermöglichen, gibt es verschiedene Ansätze. Ein Weg besteht darin, in die Geräte zusätzlich die Technik für die bisherigen Mobilfunksysteme – etwa GSM oder UMTS – einzubauen bzw. Chipsätze zu verwenden, die beide Techniken unterstützen. Dieser „Simultaneous Voice and LTE" (SVLTE) genannte Ansatz hat für die Netzbetreiber den Vorteil, dass für die reinen Sprachdienste die vorhandenen Netze und Techniken genutzt werden können. Die Anwender müssen dafür aber einen höheren Energieverbrauch in Kauf nehmen.

Auch Circuit Switched Fallback (CSFB) löst das Problem auf technische Art. Datenübertragung erfolgt auch hier per LTE, bei Sprach- oder Kurznachrichtendiensten wird aber auf GSM- oder UMTS-Dienste zurückgegriffen. Dieses „Umschalten" der Technik kann einige Sekunden dauern, was zu Verzögerungen beim Aufbau der Verbindung führt. Zudem erfordert CSFB auf Seiten des Netzwerks Anpassungen der Schnittstelle zwischen der Vermittlungsstelle, dem sog. Mobile Switching Center (MSC), und dem Übergang zum Zugangsnetz, der sog. Mobile Management Entity (MME).

Ein anderer Weg für die LTE-Telefonie führt über IP-basierte Sprachsysteme. Anwendungen wie Skype oder FaceTime stellen solche „Voice over IP"-Dienste (kurz „VoIP") recht unkompliziert zur Verfügung. Auch wenn VoIP-Dienste nicht unbedingt kompatibel zueinander sind, erfreuen sie sich großer Beliebtheit – obwohl ihrem professionellen Einsatz zum Teil Sicherheitsbedenken entgegenstehen. Für die Netzbetreiber haben diese Dienste aber einen großen Nachteil: Sie erbringen keine wesentlichen Einnahmen, da lediglich der Datenverkehr ansteigt. Bedenkt man, dass derzeit etwa 70 % der Umsätze von Mobilfunkbetreibern über die Telefonie erzielt werden – immerhin weltweit etwa 500 Milliarden Euro pro Jahr – wird verständlich, dass die Unternehmen versuchen, dieses Geschäft für sich zu sichern.

Eine echte Integration von Telefonie in LTE soll durch Voice over LTE (VoLTE) erfolgen. Mit zwei Spezifikationen für einfache und für Bildtelefonie hat der Verband der GSM-Mobilfunkanbieter, die GSMA, die Standardisierung dieser Dienste in Angriff genommen. Mit VoLTE sollen die typischen Telefondienste mit besonders guter Sprachqualität bereit stehen. Heute übliche Leistungsmerkmale wie Anrufweiterleitung bzw. Unterdrückung der Weiterleitung, Anruferidentifikation oder das Halten, Rückfragen und Makeln bei Gesprächen sollen dann ebenfalls realisiert sein.

Auch für Kurznachrichten werden die modernen Leistungsmerkmale wie verknüpfte SMS oder Zustellbestätigung implementiert. Allerdings sind auch für die reibungslose Vermittlung zwischen SMS over LTE und dem üblichen SMS-Transport besondere Schnittstellen in den Netzen erforderlich: Die Nachrichten werden innerhalb LTE mit dem Protokoll Session Initiation Protocol (SIP) transportiert. Der Übergang in leitungsvermittelte Netze erfolgt über ein IP-SM-Gateway, in dem die Textnachricht aus dem SIP-Paket ausgepackt und als normale SMS weitergeleitet wird. Für eingehende SMS übernimmt das Gateway die Kapselung in ein SIP-Paket.

Die unterschiedlichen Mobilfunktechniken der zweiten und dritten Generation einerseits und der vierten Generation andererseits werfen nicht nur die Frage auf, wie Sprach- und Kurznachrichtendienste realisiert werden können, bis sie über LTE möglich sind. Auch das sog. „Hand-over" von Gesprächen stellt eine Herausforderung dar, wenn der Nutzer mit einem LTE-Handy von einer LTE-Zone in ein Gebiet wechselt, in dem die schnelle All-IP-Technik noch nicht verfügbar ist. Auch dafür wurde durch weltweite Kooperation von Standardisierungsgremien im Rahmen des 3rd Generation Partnership Projects (3GPP) ein Standard entwickelt, nämlich Single Radio Voice Call Continuity (SRVCC).

BEWERTUNG

Noch befinden sich in LTE integrierte Telefon- und Kurznachrichtendienste in der Entwicklung. Mit der Implementierung der dabei entstandenen neuen Standards und der zunehmenden Verbreitung von LTE könnten insbesondere Sprachdienste von den schnellen Funknetzen profitieren, denn dort könnten dann auch breitbandige Audiodienste wie HD Voice bzw. Full-HD Voice für optimale Klangqualität einschließlich der Unterdrückung von Störgeräuschen sorgen. Solange richtet sich der Blick jedoch darauf, was überhaupt an Sprachdiensten möglich ist. Für den Nutzer dürfte die tatsächlich im Hintergrund zum Einsatz kommende Technik uninteressant sein, solange diese den Komfort bei der mobilen Kommunikation nicht durch lange Umschaltzeiten oder erhöhten Energieverbrauch zu sehr einschränken.

Verwaltungsrelevanz: ■□□□

Umsetzungsgeschwindigkeit: ■■■■

Marktreife/Produktverfügbarkeit: ■■■■ – ■■■□

IMPRESSUM

Herausgeber
Hessische Zentrale für Datenverarbeitung
Mainzer Straße 29
65185 Wiesbaden
Telefon: 0611 340-0
Fax: 0611 340-1150
E-Mail: info@hzd.hessen.de
www.hzd.hessen.de

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

Satz
Birgit Lehr

Titellayout
ansicht kommunikationsagentur, www.ansicht.com

Druck
mww.druck und so … GmbH

Erscheinungstermin: Dezember 2012

HZD

Mainzer Straße 29 | 65185 Wiesbaden
Telefon: 06 11 340-0 | Fax: 06 11 340-1150
E-Mail: info@hzd.hessen.de | www.hzd.hessen.de