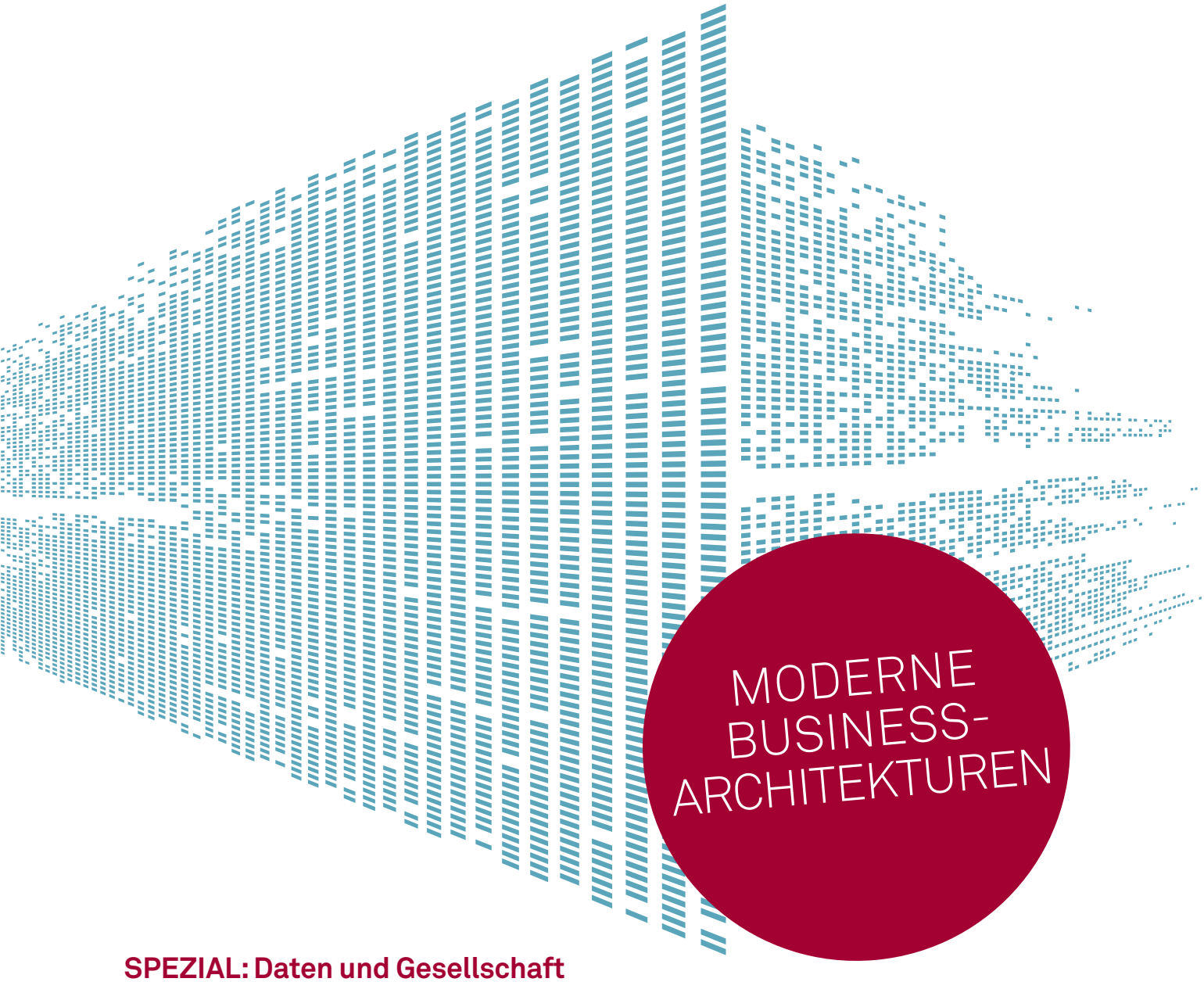
02-2020

public

Kundenmagazin der .msg
für den Public Sector

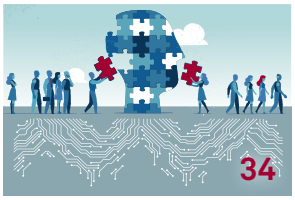


SPEZIAL: Daten und Gesellschaft

Daten für die Zukunft des Gemeinwesens

Warum die Datenwissenschaften die Sozialwissenschaften brauchen

INHALT



Herausgeber
Jürgen Fritsche, Geschäftsleitung Public Sector, msg systems ag

Robert-Bürkle-Str. 1
85737 Ismaning
Tel.: +49 89 96101-0, Fax: -1113
E-Mail: info@msg.group
www.msg.group

Verantwortlich
Dr. Stephan Frohnhoff, Rolf Kranz, Bernhard Lang, Karsten Redenius, Dr. Jürgen Zehetmaier

Redaktion
Dr. Andreas Zamperoni (Chefredakteur), Karin Dohmann, Dr. Katrin Ehlers

Konzept und Layout
Eva Zimmermann

Bildnachweis
Adobe Stock: Umschlag, S. 10, 17, 22, 27, 28, 34, 37, 42, 44, 47, 48; Bundesverwaltungsamt: S. 4, 6, 7, 9; Dr. Katrin Ehlers: S. 40; Bundesregierung S. 47

Produktion
Meisterdruck GmbH, Kaisheim

EDITORIAL

Endspurt der Redaktion bei der Erstellung unserer 17. Ausgabe der .public: Wir tragen alle Artikel im finalen Layout zusammen und legen die Reihenfolge der Artikel fest. Essenziell ist – neben anderen layouttechnischen Feinheiten –, dass die Anzahl der Seiten durch vier teilbar sein muss. Diesmal ist es eine Seite zu wenig! Ein Glücksfall, wie sich erweist: Wir sind schließlich mittendrin im derzeit spannendsten IT-Projekt der Bundesverwaltung – der Corona-Warn-App! Seit Übernahme des Projektes durch das RKI unterstützen wir das RKI und das Projekt durch vier Projektmanagerinnen und -manager. Lange Zeit sieben Tage die Woche, zwölf Stunden am Tag! Da gibt es was zu berichten! Denn die Entwicklung der Corona-Warn-App offenbart eine beeindruckende Flexibilität und Leistungskraft der öffentlichen Verwaltung, die noch weit über die bei der „Flüchtlingskrise" 2015/16 hinausgeht. Neben den coronabedingten, neuen behördlichen digitalen Arbeitsmodellen und Prozessen erkennen Bürger sowie Beraterinnen und Berater mit Genugtuung[1], was möglich ist, wenn es sein muss. Und das ist uns auf jeden Fall eine Seite (Seite 47) wert!

Viele weitere Seiten wert sind uns unsere beiden (!) Schwerpunktthemen: „Moderne Business-Architekturen" – hier lesen Sie unter anderem Beiträge über Container und Sicherheit, Architekturdokumentation und „Cassandra" – und „Daten und Gesellschaft" mit Beiträgen über die Rolle der Sozialwissenschaften für die Datenwissenschaften und – reziprok – die Rolle der Daten für die Zukunft des Gemeinwesens.

Und last but not least möchte ich Ihnen das Interview mit Christoph Verenkotte anlässlich des 60. Geburtstags des BVA, einem der Flaggschiffe der deutschen Behördenlandschaft, empfehlen.

Viel Spaß beim Lesen wünscht Ihnen

Dr. Andreas Zamperoni
Chefredakteur .public

1 https://www.youtube.com/watch?v=atAy8NGOoiw (abgerufen am 20.07.2020).

Christoph Verenkotte (Präsident BVA) im Austausch mit Jürgen Fritsche (Geschäftsleitung Public Sector, msg)

„VON A WIE AUSLÄNDERZENTRALREGISTER BIS Z WIE ZUWENDUNGEN“

Fritsche: Lieber Herr Verenkotte, das Bundesverwaltungsamt ist im Januar 60 Jahre alt geworden. Zu diesem runden Geburtstag möchten wir Ihrem Haus herzlich gratulieren. Wie feiern Sie das Jubiläum in diesen besonderen Zeiten? Oder haben Sie vielleicht schon gefeiert?

Verenkotte: Das BVA hat nach 60 aufregenden Jahren allen Grund zu feiern. Wir sind mit 299 Beschäftigten gestartet, heute sind es rund 6.000 – bundesweit an 22 Standorten. Unser Aufgabenportfolio ist enorm gewachsen und verändert sich von Jahr zu Jahr, mittlerweile bewältigen wir 150 sehr unterschiedliche Aufgaben – von A wie Ausländerzentralregister bis Z wie Zuwendungen. Wir sind für nahezu alle Bundesministerien, für Bundesbehörden, Bürgerinnen und Bürger sowie zahlreiche andere Organisationen tätig. Eine Feier kann es nun aber erst 2021 geben, das Corona-Virus hat uns einen gehörigen Strich durch die Planung unseres Festaktes mit hunderten Gästen im Jubiläumsjahr gemacht.

Fritsche: Sie selbst verbindet auch eine lange Geschichte mit dem BVA, seit zehn Jahren als sein Präsident. Welches Ereignis in all den Jahren, seit Sie 1988 zum ersten Mal eine Aufgabe im BVA wahrgenommen haben, war für Sie persönlich besonders wichtig und prägend?

Verenkotte: Das letzte Jahrzehnt war stark geprägt von mehreren Großprojekten, die das Bundesverwaltungsamt noch einmal grundsätzlich verändert haben. 2013 haben wir den Dienstleistungsbereich der Bundeswehr übernommen und in diesem Zuge

1.400 Beschäftigte an sieben neuen Standorten integriert. Mitte 2017 gab es dann einen erneuten Wachstumsschub, als wir nicht nur Dienstleistungsaufgaben des Bundesfinanzministeriums übernommen haben, sondern auch 1.500 Beschäftigte an neun Standorten. Die damit einhergehenden Veränderungen haben uns allen im BVA, aber insbesondere den betroffenen Fachbereichen eine Menge Geduld, Flexibilität, Kreativität und Lösungskompetenz abverlangt. Das haben wir sehr gut bewältigt!

In den Jahren 2015 und 2016 haben wir darüber hinaus die IT-Konsolidierung des Bundes stark unterstützt, die wir mit unserer hausinternen Bundesstelle für Informationstechnologie maßgeblich vorangetrieben haben. Aufgrund ihres Erfolges wurden alle 400 Beschäftigten der BIT in das neu geschaffene ITZBund integriert. Trotz des Verlustes von qualifizierten Leuten, den man nicht verhindern kann, bin ich stolz darauf, dass wir inzwischen im Bereich der Softwareentwicklung weiter stark aufgestellt sind und diesen ausgebaut haben.

Fritsche: Gern bescheinigt man ja der Verwaltung einen Modernisierungsstau. Wenn man aber auf 60 Jahre technische Entwicklung zurückblickt, wird doch deutlich, wie viel sich verändert hat. Welche Meilensteine der Automatisierung und Digitalisierung aus der Arbeit des BVA zeigen den Modernisierungsprozess besonders deutlich?

Verenkotte: Das Bundesverwaltungsamt hat in der Automatisierung und Digitalisierung sämtliche Veränderungen durchlebt, die auch unsere Gesellschaft prägen. Mit jedem technischen Fortschritt wurden unsere Prozesse angepasst. Sehr früh haben wir unsere Büros mit Computern ausgestattet – und zwar flächendeckend. Die BAföG-Abteilung arbeitet bereits seit Ende der 1990er-Jahre papierlos. Vom Antrag bis zum Bescheid sind die Abläufe automatisiert und mit ‚bafögonline' mittlerweile auch digitalisiert. Zunehmend digital erfolgt auch die Abwicklung der Beihilfe. Die von uns entwickelte App hat inzwischen fast 70.000 Nutzerinnen und Nutzer und erleichtert die Abrechnung enorm.

Unsere Register-Factory ist ein weiteres Beispiel beständiger Modernisierung. Das Ausländerzentralregister (AZR) ist beispielsweise mit 29 Millionen gespeicherten Datensätzen eines der größten automatisierten Register der öffentlichen Verwaltung und mittlerweile zu einer digitalen Plattform ausgebaut. Dafür wurden wir 2017 im E-Government-Wettbewerb als „Bestes Infrastrukturprojekt" ausgezeichnet. Und das ist nur ein Beispiel von vielen!

Mittlerweile sind wir für knapp 200 Behörden und Institutionen eine Art „Backoffice" und erbringen unsere Leistungen, von der Bezügeabwicklung bis zum Travel-Management, mehr und mehr voll digital.

Fritsche: Die Corona-Krise bringt viele Einschränkungen und Unsicherheiten bis hin zu Existenznot mit sich. Auf die Verwaltung, heißt es, wirke sie als Modernisierungsbeschleuniger. Vieles, was vorher lange diskutiert und vorsichtig angegangen wurde, wird jetzt in kurzer Zeit umgesetzt. Können Sie aus Sicht des BVA auch über Beispiele für die krisenbedingte Agilität der öffentlichen Verwaltung berichten?

„EINE RÜCKKEHR ZU BISHERIGEN ARBEITSWEISEN WIRD ES NICHT GEBEN."

Verenkotte: Das BVA hat sehr schnell reagiert. So viele Beschäftigte wie möglich sind ins Homeoffice gewechselt. Das BVA arbeitet schon seit Längerem daran, den Beschäftigten ein flexibles Arbeiten zu ermöglichen. Videokonferenzen wurden fast zur Standardkommunikation in der Krise – wie andernorts auch.

Fritsche: Sehen Sie darin vor allem positive Entwicklungen oder sehen Sie einige auch kritisch, zum Beispiel in punkto IT-Sicherheit?

Verenkotte: Wir erleben gerade, wie sich unsere Arbeitswirklichkeit verändert: Arbeit wird digitaler und lässt sich vielfach im Homeoffice erledigen. Besprechungen und Workshops finden im Netz statt. Das sind jetzt kurzfristige Prozesse, die langfristig begleitet werden müssen: von veränderten Arbeitsprozessen und neuen Arbeitsformen wie selbstbestimmtere Arbeitsweisen, flachere Hierarchien, verstärkter Einsatz agiler Methoden.

Allerdings brauchen solche Veränderungen Zeit. Die durch die Krise erzwungene Beschleunigung und Beschränkung auf kleinere, improvisierte Maßnahmen birgt auch die Gefahr, dass Akzeptanz verloren geht. Umso wichtiger sind jetzt schnelle Fortschritte nicht nur im Bereich der E-Akte, digitaler Eingangskanäle und Scanlösungen. Und natürlich müssen alle Entwicklungen durch Sicherheitskonzepte begleitet werden. Das versteht sich heute von selbst. Und eins ist klar: Eine Rückkehr zu bisherigen Arbeitsweisen wird es nicht geben.

Fritsche: Wie begegnen Sie als Behördenleiter der durch Corona und Digitalisierung möglicherweise potenzierten Verunsicherung der Mitarbeiterinnen und Mitarbeiter?

Verenkotte: Wir gehen davon aus, dass für viele Beschäftigte das Homeoffice ein Zukunftsmodell ist, das von den Beschäftigten sogar verstärkt eingefordert wird. Das beobachten wir jetzt schon. Ich bin der Auffassung, dass es für eine Vielzahl der BVA-Ar-

beitsplätze auf freiwilliger Basis möglich sein wird, im Homeoffice zu arbeiten. Aber selbstverständlich gibt es unter den Beschäftigten auch einige, die weiterhin einen Büroarbeitsplatz benötigen und nicht von zu Hause aus arbeiten wollen oder können. Auch diesen Menschen müssen wir gerecht werden. Unsere Führungskräfte müssen ebenfalls mitwachsen, denn Führen auf Distanz wird zum Normalfall.

Ich gehe davon aus, dass es uns gelingen wird, unsere Beschäftigten für diesen Kurs zu gewinnen. Die Technik muss natürlich in allen Bereichen stimmen, dazu gehören funktionierende und starke Netzlösungen. Das verlangen auch unsere Mitarbeiterinnen und Mitarbeiter – mit Recht.

Meine Hauptaufgabe sehe ich insgesamt darin, das BVA für die Zukunft gut aufzustellen und dafür zu sorgen, dass die Rahmenbedingungen stimmen: rechtlich, technisch, organisatorisch. Dafür setze ich mich auch in Berlin ein.

„FÜHREN AUF DISTANZ WIRD ZUM NORMALFALL."

Fritsche: Haben sich für das BVA aus der Krise neue Aufgaben ergeben?

Verenkotte: Wir haben eine ganze Reihe neuer Aufgaben übernommen. Lassen Sie mich nur einige nennen:

Beispielsweise wurden dem Bundesministerium für Gesundheit (BMG) zur Bekämpfung von COVID-19 zusätzliche Mittel zur Verfügung gestellt. Da wir seit Jahren die administrative Bearbeitung von Fördergeldern für das BMG wahrnehmen, sind wir auch in diesem Fall involviert und behandeln die Mittelvergabe mit hohem Tempo.

Dann strebt die Bundesregierung an, dass Schutzkleidung für Ärzte und medizinisches Personal zur Behandlung von COVID-19-Patienten verstärkt aus deutscher Herstellung kommt. Deshalb hat das Bundesgesundheitsministerium (BMG) entsprechende Rahmenverträge mit Lieferanten geschlossen. Ab Mitte August sollen pro Woche bis zu 50 Mio. Masken und 1 Mio. Schutzkittel ausgeliefert werden. Das BVA wickelt das Programm ab, bearbeitet die Rechnungen und ordnet die Zahlungen an.

Ein weiteres Beispiel ist die Zusammenarbeit mit dem Robert-Koch-Institut, in dessen Auftrag wir im März bundesweit über 500 „Containment Scouts" gesucht und kurzfristig gefunden haben. 11.000 Bewerbungen wurden innerhalb weniger Wochen ausgewertet. Schon seit April helfen Containment Scouts in den Gesundheitsämtern bei der telefonischen Befragung von COVID-19-Infizierten und deren Kontaktpersonen.

Fritsche: Das Jubiläum ist sicherlich auch ein Anlass, die eigene Rolle zu reflektieren und nicht nur in die Vergangenheit, sondern auch in die Zukunft zu schauen. Haben Sie in der Vorbereitung des Geburtstages neu über die Vision Ihres Hauses nachgedacht, oder steht die bereits seit längerem?

Verenkotte: Eine Strategie zielt ja immer auf die Langfristigkeit der Planung ab und es sollte regelmäßig überprüft werden, ob sie noch passt oder sich Rahmenbedingungen geändert haben, die eine Korrektur oder Anpassung erforderlich machen.

Die bisherige BVA-Strategie war als „Strategie 2018plus" bekannt. Im Jahr 2018 angekommen galt es dann, die nächste Etappe in den Blick zu nehmen. Die neue Strategie BVA 2025 priorisiert seit 2018 die Digitalisierung des BVA. 2025 wollen wir die Veränderungen umgesetzt haben. Da können wir auch 65 Jahre feiern!

Fritsche: Welche Vision hat das BVA von seiner eigenen Rolle und für die Verwaltungsmodernisierung?

Verenkotte: Mit der steigenden Zahl unserer Aufgaben und Kunden ist im Laufe der Jahrzehnte nicht nur das BVA gewachsen, sondern auch die Anforderungen seitens der Politik und der Kunden haben zugenommen. Wir sind heute der zentrale Dienstleister des Bundes, und daher gilt es, unser Dienstleistungsangebot an

Erster Hauptsitz des Bundesverwaltungsamtes in Köln (bis 1984). Das BVA ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es beschäftigt derzeit rund 6.000 Mitarbeiterinnen und Mitarbeiter. Als Partner von Bürgern, Behörden, Unternehmen und Vereinen nimmt das BVA mehr als 150 Aufgaben wahr, unter anderem das Reisemanagement, die Beihilfe- und Bezügebearbeitung sowie die Personalgewinnung.

der Nachfrage unserer Kunden auszurichten. Unsere Arbeit soll als schnell und unkompliziert wahrgenommen werden, sprich: Wir wollen unsere Kunden mehr „abholen", sie beraten und unterstützen.

Zudem sind wir bundesweit als „Beratungsinstanz" gefragt. Unser Beratungszentrum des Bundes betreut jährlich über 1.000 Projekte und berät eine Vielzahl von Kunden, darunter oberste Bundesgerichte, Sicherheitsbehörden, Einrichtungen der allgemeinen und inneren Verwaltung sowie zahlreiche Institutionen aus Wissenschaft, Politik und Kultur. Die Themen sind breit gefächert: In den Beratungen geht es um die strategische Ausrichtung, um Digitalisierung und immer auch um das entsprechende Projekt- und Prozessmanagement.

Unser Beraterteam hat zum Beispiel ein Vorgehensmodell zur Einführung der E-Akte Bund entwickelt und unterstützt Behörden bei der Einführung. Darüber hinaus haben wir immer im Blick, welche Regelungen in Gesetzen und Verordnungen uns darin einschränken, Verwaltung effizient und schnell zu gestalten. Hier gehen wir dann proaktiv auf die Ministerien zu und zeigen Lösungs- beziehungsweise Änderungsvorschläge auf.

Fritsche: Können Sie etwas zu den Eckpfeilern Ihrer Strategie sagen?

„UNSERE ARBEIT SOLL ALS SCHNELL UND UNKOMPLIZIERT WAHRGENOMMEN WERDEN."

Verenkotte: Für die kommenden Jahre lautet unsere Maxime „nachfrageorientiert, zukunftsweisend und nachhaltig". Wir wollen Verwaltung einfach, schnell und flexibel machen. Mit der weiteren Digitalisierung von Fachanwendungen werden wir einen effizienten und nachhaltigen Ressourceneinsatz sicherstellen und Lösungen für die Verwaltung der Zukunft entwickeln, die auch anderen zur Verfügung stehen. Die digitale Transformation ist dabei die Chance, Verwaltung noch effizienter und serviceorientierter zu gestalten. Dafür bietet unsere Digitale Agenda, die die Strategie 2025 umsetzt, für die kommenden Jahre eine gute Orientierung. Wir sehen vier Hebel am Werk: für unsere Kunden „digitale Services", für die Beschäftigten den Ausbau von „Digitalkompetenz", als Werkzeuge „fortschrittliche Analytik" sowie „Automatisierung und KI". Mit „Big Data" und fortschrittlicher Analytik werden wir unter anderem Fehler verringern und Entscheidungen unterstützen.

Fritsche: Welche Rolle spielen in der Strategie die Aspekte „Daten" und „künstliche Intelligenz"?

Verenkotte: Beide Bereiche spielen eine große Rolle: Mit „Big Data" und fortschrittlicher Analytik werden wir unter anderem Fehler verringern und Entscheidungen unterstützen können. Durch die Nutzung von Automatisierung und künstlicher Intelligenz entfallen beispielsweise Routineaufgaben, so dass unsere Beschäftigten wieder mehr Zeit für die persönlichen Belange unserer Kundinnen und Kunden hätten. Hier ist noch erhebliches Potenzial.

Fritsche: Welche Rolle spielt das BVA in der Umsetzung von „Once only", also der Vorgabe, dass Bürger oder Unternehmen ihre Daten nur einmal eingeben müssen und die Verwaltung bedarfsweise auf diesen Datenbestand zugreifen kann?

Verenkotte: Seit 2017 ist das BVA an dem Horizon-2020-Projekt zur Erforschung der Machbarkeit des Once-only-Prinzips beteiligt – auch bekannt als TOOP: The Once-Only Principle Project. Es ist ein Gemeinschaftsprojekt von BMI, der Universität Koblenz-Landau und der Metropolregion Rhein-Neckar zur Entwicklung einer IT-Architektur. Diese Architektur soll es innerhalb der EU-Mitgliedstaaten ermöglichen, in einer behördlichen Einrichtung bereits gespeicherte Daten für Behörden anderer Mitgliedsländer einmalig zur Verfügung zu stellen.

Fritsche: Welche Voraussetzungen müssen dafür geschaffen werden?

Verenkotte: Eine der wesentlichen Voraussetzungen für die Nutzung bereits gespeicherter Daten ist es, die verschiedenen Systeme interoperabel – also kompatibel – zu gestalten. Gerade für die föderale Struktur in Deutschland mit ihrer dezentralen Registerlandschaft stellt dies die größte Herausforderung dar.

Wichtig wird auch die Authentifizierung und Identifizierung der Datenbesitzer. Nur sie sollten die Zustimmung zur Bereitstellung der Daten aus einem System zu einem anderen erteilen. Hierfür müssen sich Nutzerinnen und Nutzer allerdings eindeutig identifizieren können. Das BMI entwickelt dazu gerade ein Nutzerkonto – eine dringend erforderliche Lösung.

Fritsche: Welche Aufgaben werden bei der Umsetzung der Datenstrategie des Bundes (siehe auch Infobox) auf das BVA zukommen?

Verenkotte: Seit Inkrafttreten des sogenannten Open-Data-Gesetzes (§ 12a EGovG) leistet das BVA einen wichtigen Beitrag zur Bereitstellung von Daten in der Bundesverwaltung. Unser Kompetenzzentrum Open Data sorgt für Kompetenzaufbau und übernimmt Koordinierungsaufgaben innerhalb der Bundesverwaltung und zwischen den zuständigen Stellen der Länder. Wir schaffen so ein Netzwerk zwischen den jeweiligen Open-Data-Akteuren und planen aktuell einen runden Tisch mit dem Ziel des Bund-Länder-Austauschs.

Das BVA leistet zudem schon jetzt seinen eigenen Beitrag zur Bereitstellung von offenen Daten, ganz im Sinne der Datenstrategie der Bundesregierung. Da geht es natürlich um BVA-originäre Daten und nicht um die Daten unserer Kundenbehörden, die nur von den Kunden selbst bereitgestellt werden können. Der Prozess der Identifikation solcher Daten im BVA wird vom Kompetenzzentrum intensiv begleitet. Ganz sicher wird Verwaltungshandeln in der Zukunft durch Open Data verändert: Welche zusätzlichen Aufgaben daraus entstehen, bleibt abzuwarten.

Fritsche: Welche Konzepte zu Datenschutz und Datensicherheit verfolgen Sie dabei?

Verenkotte: Das Kompetenzzentrum Open Data ist auf dem Feld der Bereitstellung von Verwaltungsdaten als offene Daten tätig. Es findet keine rechtliche Prüfung der Datenbestände Dritter statt. Ob ein Datensatz geeignet ist, muss die umsetzende Behörde entscheiden. Allerdings liefert ein Leitfaden des Kompetenzzentrums eine Art Prüfschema, in dem Anhaltspunkte zur Rechtmäßigkeit und Empfehlungen enthalten sind. Dies ersetzt aber nicht die rechtliche Prüfung.

Fritsche: Welche Bedeutung hat das Thema KI für eine Behörde wie das BVA?

Verenkotte: Das Thema künstliche Intelligenz wird aktuell auf allen gesellschaftlichen Ebenen diskutiert. Dass die KI in den Bereich der öffentlichen Verwaltung Einzug hält und eine Behörde wie das Bundesverwaltungsamt hier aktiv wird, ist nur folgerichtig. Wir wollen und werden KI nutzen, aber in vielen Fällen muss erst noch die Automatisierung vorangetrieben werden. Anwendungsfälle gibt es, und wir prüfen die nächsten Schritte.

„KI-ERGEBNISSE MÜSSEN NACHVOLLZIEHBAR SEIN."

Fritsche: Welche KI-Themen sind für Sie grundsätzlich interessant und umsetzbar?

Verenkotte: KI kann jetzt schon im Bereich der Bilderkennung einen großen Mehrwert bringen. Hier sind unterschiedliche Szenarien denkbar: Bei der Massenverarbeitung von Textdokumenten

DATENSTRATEGIE DER BUNDESREGIERUNG

Gemäß den Eckpunkten zur Datenstrategie möchte die Bundesregierung den Bund als Vorreiter und Treiber einer verstärkten Datennutzung und Datenbereitstellung etablieren. Dazu will die Bundesregierung unter anderem: a) die Nutzbarmachung, Vernetzung und Analyse öffentlich finanzierter Datensätze verbessern (Open Data), b) Maßnahmen und Instrumente zur Erhöhung der Datenkompetenz im Sinne einer umfangreichen „Data Literacy" in den Bundesbehörden prüfen und initiieren, c) die Potenziale der Datennutzung für eine effizientere und bürgerfreundlichere Aufgabenerfüllung staatlicher Einrichtungen heben, d) gesicherte Verbindungen zur Übermittlung von Daten innerhalb der öffentlichen Verwaltung zur ebenenübergreifenden Zusammenarbeit schaffen und auch weitere Maßnahmen der Datensicherheit prüfen sowie e) Maßnahmen zur Verbesserung einer ökologisch und digital nachhaltigen Dateninfrastruktur in den Bundesbehörden prüfen und initiieren.

können beispielsweise leicht zu erfassende Informationen maschinengestützt extrahiert und für die Weiterverarbeitung vorbereitet werden. Im Bereich des 1st-Level-Supports – also bei Help-Desk-Systemen – sind automatisierte Klassifizierungen von E-Mail-Anfragen heute schon möglich.

Fritsche: Sind Sie zum Thema KI im Austausch mit anderen Behörden, um etwa Leitlinien zu setzen, gemeinsam etwas zu entwickeln bzw. voneinander zu lernen?

Verenkotte: Gerade im Bereich KI ist das Interesse an einem projektbezogenen Austausch sehr groß. So werden Leitlinien, die innerhalb des BMI erarbeitet werden, auch mit anderen Behörden abgestimmt. Da geht es zum Teil um ethische Fragen, aber vor allem um technologische Grundsätze. Im BVA befürworten wir beispielsweise die Verwendung von Open-Source-Software, also müssen wir sicherstellen, dass der Quellcode von Software keine schädlichen Funktionen beinhaltet oder ungewünschte Ausleitungen von Daten möglich sind.

Fritsche: In welchem Stadium der Entwicklung von KI-Anwendungen sind Sie?

Verenkotte: Die Verwendung von KI darf kein Selbstzweck sein, sondern ist immer ein Puzzleteil innerhalb einer Anwendungslandschaft. Hier ist das Bundesverwaltungsamt gut aufgestellt, da wir grundsätzlich bei der Software-Architektur auf Anpassbarkeit, Wiederverwertbarkeit und Nachhaltigkeit achten. Wir evaluieren KI-Anwendungen, um den qualitativen Mehrwert auch quantifizieren zu können.

Fritsche: Welche Maßnahmen ergreifen Sie, um diskriminierungsfreie Ergebnisse zu erzielen?

Verenkotte: Unser höchstes Ziel ist es, bei der Auswahl der KI-Komponenten und Daten im kompletten Software-Lifecycle mögliche Diskriminierungsgefahren zu berücksichtigen. So dürfen bei der Auswertung von personenbezogenen Daten keine Personengruppen benachteiligt werden. KI-Ergebnisse müssen nachvollziehbar sein. Darauf legen wir größten Wert. Grundsätzlich gilt, dass kritische Entscheidungen aufgrund von statistischen, maschinell ermittelten Wahrscheinlichkeiten immer noch von Menschen durchzuführen und zu bewerten sind.

Fritsche: Gibt es bereits erste Erfolge?

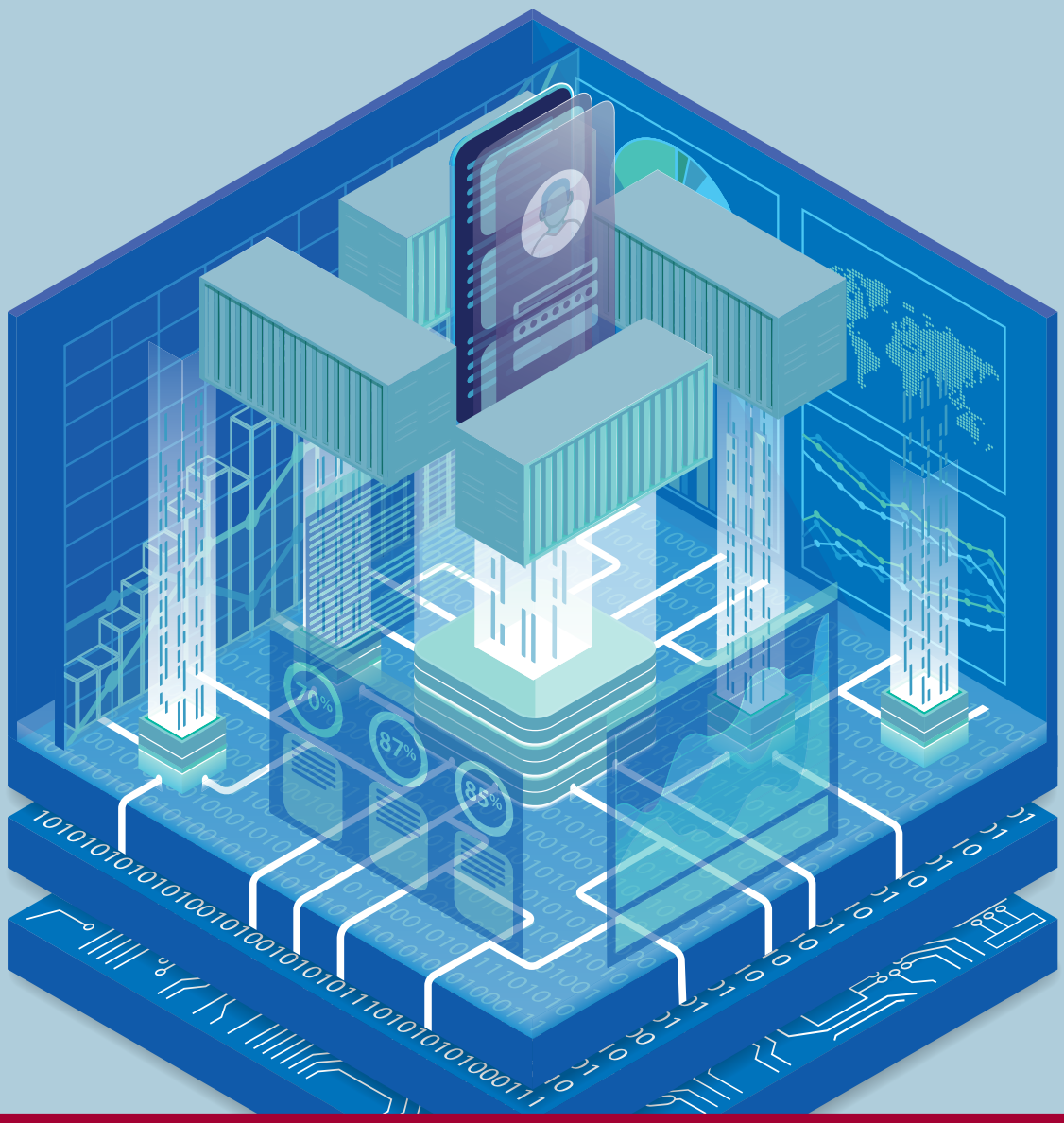
Verenkotte: Ein wichtiges Thema in der Behördenwelt ist natürlich die Datenanalyse, die vorrangig operationalisiert werden soll. Bei Datenqualitätsanalysen beispielsweise testen wir bereits entsprechende Methoden, um schneller Fragen aus dem Bereich der Politik beziehungsweise der Partnerbehörden zu den von uns verwalteten Daten liefern zu können. Da sind wir auf einem sehr guten Weg.

Fritsche: Wo sehen Sie den größten Wert der KI für die Zukunft des BVA beziehungsweise seiner Kunden?

Verenkotte: KI kann einen wertvollen Beitrag leisten, um Verwaltungsprozesse zu vereinfachen und zu automatisieren. Wichtig ist, dass sie unterstützend eingesetzt wird. Dann werden sowohl die Beschäftigten als auch die Kunden ihren Mehrwert klar erkennen. Wichtig ist natürlich der sensible Umgang mit Daten und ein klares Gerüst rechtlicher und ethischer Rahmenbedingungen.

Fritsche: Was sind nächste wichtige Meilensteine beziehungsweise Aufgaben für das Bundesverwaltungsamt?

Verenkotte: Man kann es nicht oft genug sagen: Digitalisierung, Digitalisierung, Digitalisierung. Unsere Kunden erwarten die digitale Erreichbarkeit der Dienstleistungen, unsere Beschäftigten erwarten die technische Ausstattung. In fünf Jahren sollen alle relevanten Verwaltungsverfahren im BVA digital gestaltet sein. Für diese Aufgaben brauchen wir qualifizierte Mitarbeiterinnen und Mitarbeiter. Unsere Personalplanung muss die zukünftigen Anforderungen widerspiegeln; Personalgewinnung, -bindung und -entwicklung müssen angepasst werden. Den demografischen Wandel, der uns in den kommenden Jahren erfasst – 40 Prozent unserer Beschäftigten verabschieden sich bis 2030 in den Ruhestand –, sehe ich als große Herausforderung. Schnelle und konsequente Digitalisierung ist daher unsere einzige Chance! ●



CONTAINER UND SICHERHEIT

| von DR. ROGER FISCHLIN

Sie nutzen eine bekannte Suchmaschine? Oder sehen Filme bei einem populären Video-Streaming-Dienst? Dann haben Sie, vielleicht ohne es zu wissen, bereits Container-Technologie genutzt. Andere Unternehmen, auch die IT der öffentlichen Hand, setzen inzwischen ebenfalls vermehrt auf containerbasierte IT-Lösungen. Doch mit der Container-Technologie gehen neue Bedrohungen für die Informationssicherheit einher.

NEUE TECHNOLOGIE, BEKANNTE HERAUSFORDERUNGEN

In den Augen vieler zunächst eine einfache Variante der Rechnervirtualisierung hat die Container-Technologie die Architektur von IT-Fachverfahren und deren Betrieb heute grundlegend verändert: Anwendungen sind kein Monolith mehr, sondern das Zusammenspiel von vielen Mikroservices. Anwendungen werden nicht mehr installiert, sondern Container-Images zentral bereitgestellt. Anwendungen werden nicht mehr gestartet, sondern Container orchestriert. Dies schafft auch eine Voraussetzung für die agile Entwicklung und „Continuous Delivery", um schneller auf Anwenderwünsche reagieren zu können.

Doch mit der Container-Technologie gehen neue Bedrohungen für die Informationssicherheit einher. In diesem Beitrag skizzieren wir diese Technologie, beleuchten die Risiken und erläutern, wie man ihnen entgegenwirkt. Die Grundsätze der Informationssicherheit haben in der Container-Welt Bestand. Es sind die bekannten Herausforderungen für Vertraulichkeit, Integrität und Verfügbarkeit. Doch die Maßnahmen muss man auf die neuen Herausforderungen ausrichten.

DER NEUE ANSATZ: MIKROSERVICES, CONTAINER UND ORCHESTRIERUNG

Das Design von IT-Fachverfahren folgt seit über einem Jahrzehnt der Drei-Schichten-Architektur (Three Tier Architecture):

- Webserver als Frontend beziehungsweise User Interface (Präsentationsschicht)
- Applikationsserver mit der Logik (Mittelschicht)
- Relationale Datenbank als Backend (Persistenzschicht)

Es ist ein lineares Modell: Anwender kommunizieren mit dem Webserver, dieser mit dem Applikationsserver und dieser seinerseits mit der Datenbank. Der Webserver bereitet die Informationen für den Nutzer auf, verarbeitet werden die Daten ausschließlich auf dem Applikationsserver. Für die dauerhafte Datenhaltung (Persistenz) nutzt dieser eine Datenbank.

Der Three-Tier-Ansatz mit einem komplexen Applikationsserver ist ungeeignet für die agile Entwicklung mit ihren fortlaufenden kleinen Anpassungen. Vielmehr ist es wegen der Abhängigkeiten eher erforderlich, Änderungen in größere Releases zu bündeln. Für ein zeitnahes „Continuous Delivery" (CD) entkoppelt man Verfahren heute in Teildienste, sogenannte Mikroservices, mit definierten Schnittstellen. Eine Änderung betrifft meist nur die Implementierung eines Mikroserviceses, nicht das Zusammenspiel mit den anderen Diensten. Die Kapselung mit definierten Schnittstellen erleichtert darüber hinaus, vorhandene Microservices in anderen Anwendungen einzusetzen oder von Dritten angebotene Komponenten zu verwenden.

Das typische Mikroservice-Design besteht aus einem zentralen API-Gateway, auch Edge-Service genannt. Über ihn kommuniziert der Nutzer beziehungsweise der Webserver (allgemeiner das User-Interface) mit den internen Mikroservices. Die zentrale Schnittstelle erlaubt, Authentifizierung usw. für alle Anfragen an Mikroservices einheitlich zu regeln. Ein bekannter Vertreter ist „Zuul" des Streaminganbieters Netflix[1]. Der Streaming-Dienst nutzt das API-Gateway, das in Release 2 Open-Source ist, für seine Angebote. Cineasten erkennen im Namen die Anspielung auf den Film Ghostbusters.

Es liegt nahe, Mikroservice mit Container gleichzusetzen. Doch ein Mikroservice ist vielmehr ein Dienst, der aus mehreren Containern bestehen kann, etwa einem Applikationsserver und einer Datenbank. Das Ziel von Mikroservices sind per se nicht möglichst kleine Dienste, sondern in sich geschlossene Systeme. Wolff charakterisiert dies in seinem Buch „Microservices – Ein Überblick"[2] wie folgt:

- Ein Team sollte den Mikroservice entwickeln und pflegen können.
- Die Funktionalität des Mikroservices sollte für das Team überschaubar sein.
- Ein Mikroservice sollte innerhalb der Anwendung ersetzbar sein.

Schlüssel des Designs mikroservicebasierter Anwendungen ist es, Komponenten ersetzen zu können.. Je kleiner ein Mikroservice ist, desto leichter ist er auszutauschen. Allerdings gibt es praktische Hindernisse:

- Programmlogik kann nur bedingt über Mikroservices hinweg verschoben werden.
- Fachliche Konsistenz der verarbeiteten Informationen lässt sich leichter innerhalb eines Mikroservices sicherstellen.
- Jeder Mikroservice benötigt als unabhängige Komponente eine eigene Umgebung.

Neu ist die Entkopplung von Diensten indes nicht. Sie war unter dem Schlagwort „serviceorientierte Architektur" (SOA) bereits um die Jahrtausendwende populär. Die Schnittstellen waren jedoch komplex: Die Services sollten nicht direkt, sondern organisationsübergreifend über einen Enterprise-Service-Bus kommunizieren.

Mit der Container-Technologie ist jetzt der nächste Schritt hin zur Kapselung einer Anwendung auf Basis von Mikroservices möglich.

CONTAINER STATT EINZELNER RECHNER

Ein Container enthält ein Programm mitsamt allen Abhängigkeiten, wie Bibliotheken, Hilfsprogrammen und statischen Daten. Man spricht von Anwendungsvirtualisierung, denn ein Container ist kein vollständiger Rechner mit eigenem Betriebssystem (Kernel). Weil Container in sich abgeschlossen sind, lassen sich Altverfahren (Legacy-Systeme), die bestimmte Versionsstände von Programmen erfordern, so auf modernen Rechnern betreiben.[3]

Die Hauptanwendung von Containern ist indes die Gliederung von Anwendungen in einzelnen Services. Ein (Anwendungs-)Container ist dabei „ein Konstrukt zum Paketieren und Ausführen einer Anwendung oder ihrer Komponenten, die auf einem gemeinsam genutzten Betriebssystem ausgeführt werden".[4]

Bei der Rechnervirtualisierung wird die gesamte Hardware des Rechners auf dem Gastsystem (Wirt) nachgebildet. Dabei erfordert jede virtuelle Maschine ein separates Betriebssystem. Bei Containern separiert man die Ressourcen zwischen Containern dagegen auf Betriebssystemebene des Wirts. Jeder Container hat einen eigenen Blick auf Ressourcen wie Prozesse, Netzwerk, Nutzer und Dateisystem. Container benötigen so im Vergleich zu virtuellen Rechnern deutlich weniger Ressourcen, man kann sie signifikant schneller starten und stoppen. Erkauft wird dieser Vorteil durch einen Rückschritt bei der Virtualisierung und mehr gemeinsamen Ressourcen. Auf virtuelle Rechner wird dennoch nicht verzichtet, oft laufen die Container auf virtuellen Maschinen.

Populär wurde die Container-Technologie mit dem Produkt der Firma „Docker" vor rund fünf Jahren. „Docker" ist zum Gattungsbegriff geworden. Es gibt zwar mittlerweile auch andere Container-Lösungen, sie spielen aber bisher noch nur eine untergeordnete Rolle.

Eine Container-Engine steuert die Container auf einem Rechner. Ein Container wird über ein Image, eine Datei mit einem Speicherabbild, initiiert. Die Engine speichert Änderungen des Containers an dessen Filesystem in einem Overlay-Dateisystem (vergleichbar mit Deltainformationen nach Snapshots). Beim Neustart des Containers sind diese Informationen gelöscht, er startet wieder mit dem Image. Veränderungen oder gar böswillige Manipulationen am Container „überleben" einen Neustart nicht – im Gegensatz zu einer virtuellen Maschine mit ihrem eigenen Dateisystem. Für dauerhaft zu speichernde Informationen (Persistenz) verwenden Container externe Speich-

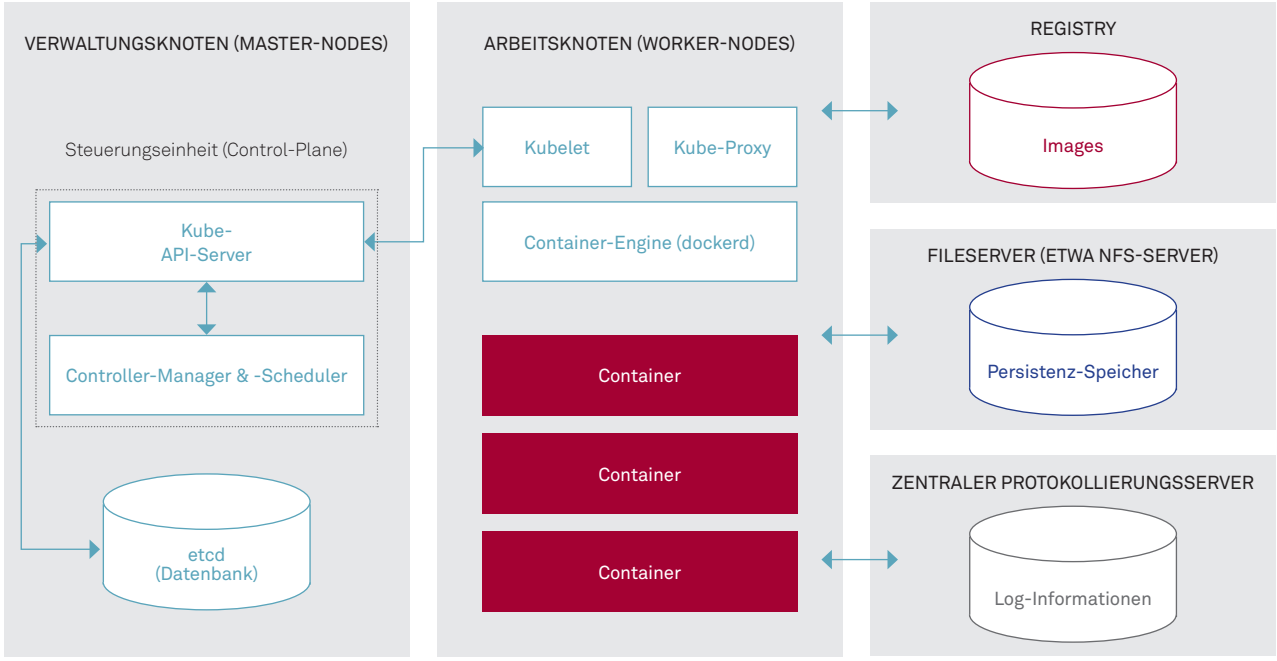


Abbildung 1: Aufbau Kubernetes-Cluster

erorte (Persistent-Volumes, PV) wie NFS-Shares oder nutzen externe Datenbanken. Logeinträge leitet ein Dienst an einen zentralen Protokollierungsserver weiter.

Die Images werden bei einer Docker-Installation in einer webbasierten Registry vorgehalten, um bei Bedarf neue Container zu initiieren. Images sind portabel, von anderen erstellte Images sind im Grundsatz auf vergleichbaren Betriebssystemen funktionsfähig. Eine große Auswahl von Images zu freier Software gibt es im Internet, beispielsweise im „Docker Hub". Allerdings ist die Qualität der Images nicht immer überzeugend, und es besteht die Gefahr verborgener Programme (Schadsoftware, Kryptominer usw.), weshalb Docker in seiner Bibliothek „Docker Store" nur qualitätsgesicherte Images anbietet.

Wer Container auf einem einzelnen Rechner laufen lässt, nutzt im Wesentlichen nur die Trennung der Anwendungen und das einfache Update mittels aktualisierter Images. Das Potenzial der Technologie für ausfallsichere und skalierbare Verfahren zeigt sich erst, wenn man für die Container einen Pool von Servern nutzt. Einen solchen nennt man Cluster, dessen Mitglieder Knoten (Nodes). Die Steuerung (Orchestrierung) der Container ist händisch nicht mehr zu bewerkstelligen. Vielmehr übernimmt ein Scheduler die Verteilung der Container auf den Knoten. Er ist Teil eines Orchestrators, der autonom den Betrieb der Container auf dem Cluster steuert.

Der heute zweifellos populärste Orchestrator, Kubernetes, stammt von Google. Ursprünglich unter dem Namen Borg vor 15 Jahren für den reibungslosen Betrieb ihrer Suchmaschine entwickelt ist Kubernetes heute das Tool für die Container-Orchestrierung, die auf Docker oder anderen Container-Lösungen aufbaut. Für tiefergehende Informationen wird auf das Kubernetes-Einführungstutorial verwiesen.[5]

SICHERHEIT

Übersicht

Die Container-Technologie bietet, wie bereits erwähnt, zahlreiche Vorteile, birgt gleichwohl auch Risiken für die Informationssicherheit. Die Container-Virtualisierung bedeutet letztlich einen Schritt zurück von der Rechnervirtualisierung. Die wesentlichen Ereignisse, die man bei Anwendung der Container-Technologie verhindern beziehungsweise deren Auswirkungen man einschränken muss, sind:

- **Trojaner im Image:** Es wird unbemerkt ein bösartiges (malicious) Image für einen Container genutzt, der so unerwünschte Aktivitäten entfaltet.
- **Schwachstelle im Image:** Es wird unbemerkt ein Image mit veralteter Software für einen Container genutzt, dessen Schwachstelle einem Angreifer erlaubt, den Dienst beziehungsweise den Container anzugreifen.
- **Container-Breakout:** Ein im Container laufendes Programm bricht aus seiner Umgebung aus und greift – unter Umgehung der Schutzmechanismen – andere Container, deren Daten (auf Persistent-Volumes oder in Datenbanken), den Knoten oder gar das gesamte Cluster an.
- **Orchestrator-Angriff:** Ein Unberechtigter manipuliert den Orchestrator oder Teile davon und greift so die Anwendungen des Clusters an.

Diese Szenarien sind durchaus real. Sicherheitsexperten entdeckten 2018 mehrere Images auf „Docker Hub", die einen Cryptominer enthielten und millionenfach heruntergeladen wurden. Ein Jahr später wurde eine Schwachstelle in einer von Docker genutzten Komponente bekannt, die es ermöglichte, Root-Zugriff auf den Knoten aus einem mit privilegierten Rechten laufenden Container in Verbindung zu erlangen.[6] In der Fachliteratur werden als Sicherheitsstandards für Container und Orchestrierung üblicherweise zwei Quellen genannt:

- NIST Standard SP 800-190 „Application Container Security Guide"[7]
- CIS-Prüflisten für Docker und Kubernetes[8]

Die Dokumente sind kostenlos im Internet erhältlich, die Listen des Centers for Internet Security (CIS) jedoch erst nach Registrierung. NIST beschreibt Risiken für die Komponenten einer Container-Plattform und gibt abstrakt und produktunabhängig Maßnahmenempfehlungen. CIS hat für Docker und Kubernetes detaillierte Hinweise für sichere Einstellungen zusammengestellt, ergänzt um die Prüfbefehle. Das BSI arbeitet aktuell an einem IT-Grundschutz-Baustein, dessen zweiter Community Draft im Mai die Kommentierungsphase abgeschlossen hat.

Generell gilt: Mit Containern ändert sich die Art und Weise grundlegend, wie Anwendungen betrieben werden. NIST betont daher, Betriebskultur und Abläufe auf den sicheren Betrieb von containerisierten Anwendungen anzupassen. Dies gilt insbesondere für den Deployment-Prozess, denn technisch ist ein falsches oder gar manipuliertes Image schnell in die Produktion ausgerollt, wie die beiden Beispiele oben zeigen.

Containerisierte Anwendung

Voraussetzung für den sicheren Betrieb einer containerisierten Anwendung ist, dass diese die Orchestrierung unterstützt, so-

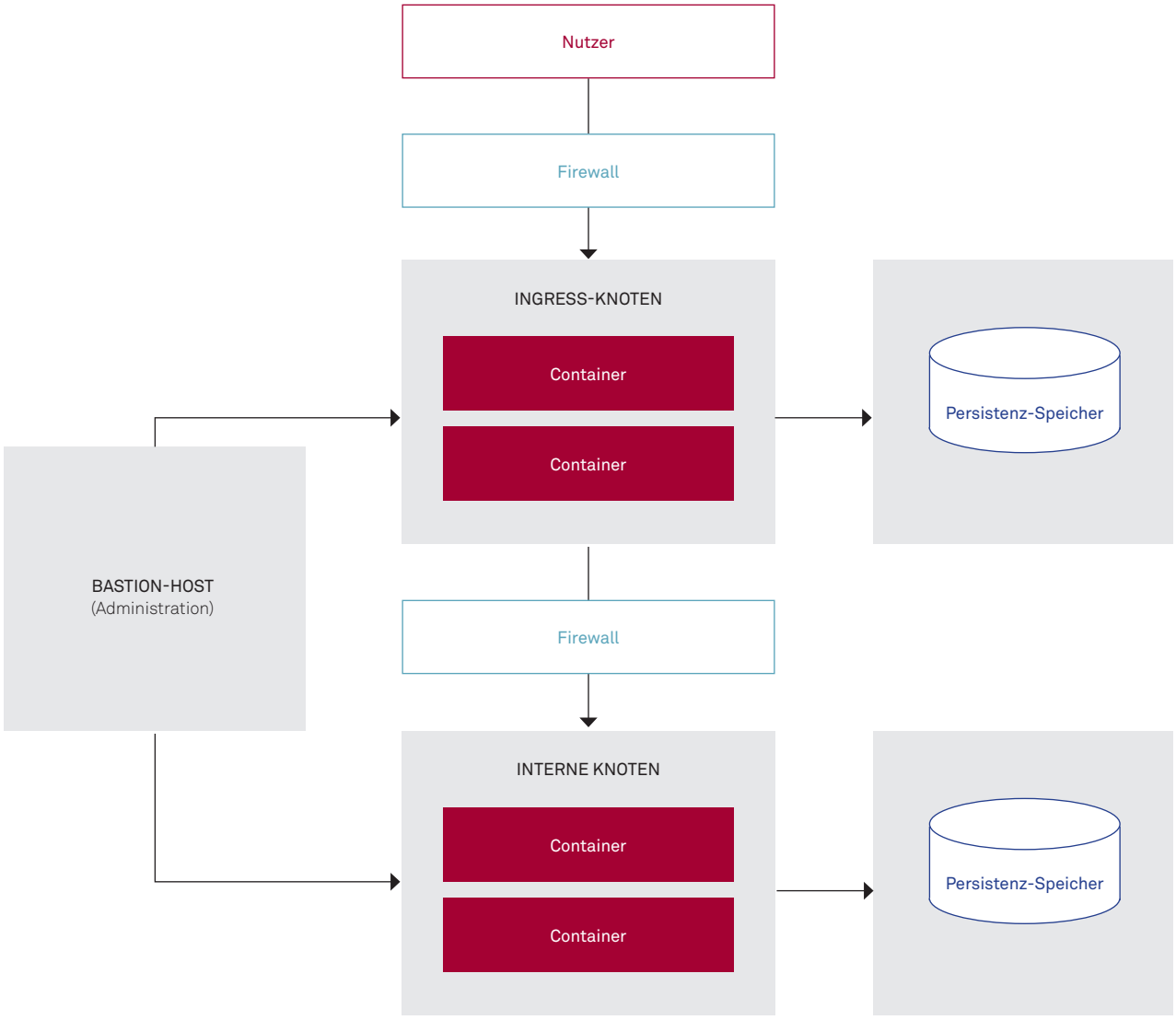


Abbildung 2: Unterteilung der Knoten

wohl vom Design als auch von der Dokumentation (Konfiguration) für den Betrieb.

Die Anwendung muss so gestaltet sein, dass der Orchestrator jeden Container beliebig neu starten kann. Unter Fachleuten ist dieser Punkt für Datenbanken umstritten: Einige argumentieren, heutige Datenbanksysteme können mit Neustarts ohne Weiteres umgehen, andere verweisen auf schlechte Erfahrungen in bestimmten Szenarien. Die Wahrheit liegt wohl dazwischen und hängt von dem Nutzungsprofil ab. Wer auf Nummer sicher gehen will, greift auf klassische Datenbankserver außerhalb des Clusters zurück.

Images

Images sind die neuen Softwarepakete, und so gelten für sie die bekannten Sicherheitsanforderungen. Man darf folglich Images nur aus vertrauenswürdigen Quellen und erst nach Integritätstest nutzen, egal ob man diese direkt verwendet oder als Basis für eigene Images nimmt. Es sollte erwogen werden, Images komplett selbst zu bauen, um unerwünschte Zusatzprogramme, Hintertüren oder Schadcodes von vornherein auszuschließen. Außerdem sollten Images versioniert und entsprechend gekennzeichnet (getaggt) sein, etwa Major Release für Funktionsänderungen und Minor Release für Bugfixes, da-

mit beim Update im laufenden Betrieb keine inkompatiblen Releases von Images zum Einsatz kommen. Die Software in Images muss regelmäßig auf bekannte Schwachstellen geprüft werden. Gleiches gilt für Schadprogramme in Images. Gerade im Kontext „Continuous Delivery" sollten diese Tests als Quality-Gates automatisiert werden. Durchgefallene Images dürfen nicht in die nächste Stufe der Pipeline gelangen. Ein populäres Programm ist „SonarQube"[9], das Komponenten in Images anhand der CVE-Meldungen auf bekannte Schwachstellen abgleicht und die Ergebnisse (Findings) gewichtet.

Ein Image darf nur die erforderlichen Pakete enthalten und keinesfalls Entwickler- oder Debugging-Werkzeuge. Remote-Zugänge (wie SSH) gehören nicht in Images. Der Zugriff in einen Container erfolgt stets über den Gastrechner. Die Software ist nach Best Practices zu konfigurieren. Images dürfen im Grundsatz keine privilegierten Rechte auf dem Gastsystem zur Ausführung benötigen. Genauso wenig wie man geheime Zugangsdaten in Quellcodes schreibt, gehören vertrauliche Informationen im Klartext in Images.

Plattform-Verantwortliche sollten die Anforderungen an Images – vor allem bei Fremdnutzung oder Mehrmandantenplattformen – dokumentieren und deren Einhaltung vor dem Deployment und danach regelmäßig prüfen. Moderne Sicherheitswerkzeuge für Container bieten umfassende automatisierte Tests für Images und ihren Inhalt (Compliance).

Registry

Registrys sind vergleichbar zu Software-Depots, daher gelten für sie die bekannten Regeln. Der Zugriff muss beispielsweise authentifiziert und autorisiert werden. Nur Berechtigte dürfen Images für die Produktion freigeben. Es gilt, den lesenden Zugriff auf relevante Personen und Systeme zu begrenzen – auch, um nicht versehentlich urheberrechtlich geschützte Software zu verbreiten. Der Zugriff auf die Registry sollte gesichert erfolgen, etwa per HTTPS.

Einen gravierenden Unterschied gibt es freilich: Bei Software-Depots stößt der IT-Betrieb die Installation an, bei Registrys zieht sich Kubernetes automatisch bei jedem Start eines Containers das passende Image. So können sich unerwünschte Images schnell verbreiten, seien es bewusst manipulierte (malicious) oder veraltete Images (Stale Images). Daher müssen Prozesse für das Deployment, Freigabe und Kontrolle der Images in der Registry etabliert werden. Man sollte prüfen, für Produktion und Test getrennte Registrys zu nutzen. Images sollten stets aus der Registry anhand eines bestimmten Funktionsumfangs (beispielsweise Major Release) in Verbindung mit aktuellen Bugfixes (Minor-Release) gezogen werden. Auf keinen Fall darf einfach die letzte verfügbare Version (latest) angefordert werden. Images dürfen nur von einer autorisierten Registry geladen werden, auch nicht aus dem Zwischenspeicher von Kubernetes. Der Zugriff auf andere Registrys sollte etwa durch Firewall-Regeln blockiert werden.

Orchestrator (Kubernetes)

Der Orchestrator muss eine sichere Umgebung für die containerisierten Anwendungen bereitstellen. Dazu gehört die Absicherung der Steuerung, ein Vertrauensverhältnis zwischen den Knoten des Clusters sowie eine Kontrolle der Kommunikation zwischen Containern.

Der Orchestrator steuert das Cluster – wer also den Orchestrator übernimmt, hat die Kontrolle über sämtliche Anwendungen auf der Container-Plattform. Wie üblich muss man daher die administrativen Zugriffe absichern und einschränken. Die von Kubernetes' standardmäßig angebotenen anonymen und ungesicherten Zugänge auf den API-Server sind zu deaktivieren. Kubernetes' einfaches Identitäts- und Berechtigungsmanagement sollte mittels Erweiterungen durch eine rollenbasierte Zugriffskontrolle (RBAC) ersetzt werden. Die Zugriffe der Agenten „Kublet" auf den Arbeitsknoten müssen gleicherweise gesichert werden. Umgekehrt muss man die Möglichkeiten von Kublet, über die zentrale API-Schnittstelle den gesamten Cluster zu steuern, einschränken.

Besonders beim Mehrmandantenbetrieb müssen Mindeststandards für den sicheren Betrieb definiert werden. Kubernetes bietet mit Security Policys die Möglichkeit, Sicherheitsvorgaben der Container-Konfiguration festzulegen, ohne deren Einhaltung der Orchestrator den Container nicht startet.

Das Overlay-Netz muss abgesichert werden. Die Kommunikation zwischen Containern sollte verschlüsselt werden, sei es auf Anwendungs-, Service-Mesh-[10] oder Server-Ebene. Ein weiterer Aspekt ist die Reglementierung des Netzverkehrs. Bei der klassischen Architektur übernehmen Firewalls diese Aufgabe. In Kubernetes' Overlay-Netz gibt es dafür Regeln in Network Policys, vorausgesetzt, das eingesetzte Netzwerk-Plug-in unterstützt diese. Da mit detaillierten Network Policys die Komplexität ansteigt, bieten bessere Sicherheitswerkzeuge an, in einer Lernphase die zulässigen Kommunikationsbeziehungen zu bestimmen und Regelsätze zu generieren. Solche Tools ermöglichen, analog zu Network-Intrusion-Detection-Systemen (NIDS) für klassische Netze, auffälligen Traffic in Overlay-Netzen zu erkennen und automatisiert verdächtige Container zu stoppen.

Die Konfiguration des Orchestrators sollte, etwa mit der CIS-Liste, regelmäßig auf Schwachstellen geprüft werden. Moderne Sicherheitslösungen für Container bieten teilweise an, die Anforderungen automatisiert abzugleichen (Audit).

Container-Laufzeitumgebung (Docker)

Ein Angreifer, der einen Container infiltriert hat, sollte zumindest nicht wieder aus diesem ausbrechen können. Dafür müssen zunächst Schwachstellen in der Container-Laufzeitumgebung vermieden werden. Der Container darf grundsätzlich nicht unter Root-Privilegien laufen oder diese erreichen können. Seine Rechte (zum Beispiel in den Linux Kernel Capabilities) müssen begrenzt sein. Eine Übersicht über die erforderlichen Capabilities findet sich im Whitepaper der „NCC Group“[11]. Der Container darf nicht den globalen Namensraum des Wirts sehen. Fachleute raten, auf dem Betriebssystem ein Security-Modul wie SELinux bei Red-Hat-Linux einzusetzen. Den von Containern ausgehenden Netzwerkverkehr gilt es zu begrenzen, damit ein Hacker abgegriffene Daten nicht nach außen senden kann.

Die Konfiguration der Container-Laufzeitumgebung sollte etwa mit der CIS-Liste regelmäßig auf Schwachstellen hin geprüft werden. Moderne Sicherheitslösungen für Container bieten teilweise an, die Anforderungen automatisiert abzugleichen (Audit).

Knoten und Betriebssysteme

Die Betriebssysteme für die Knoten müssen gehärtet sein: Plattformfremde Anwendungen oder Endbenutzer-Accounts gehören nicht auf die Server. Das Betriebssystem und dessen Administration müssen auf den Container-Betrieb ausgerichtet sein, zumal Kubernetes tief in die Interna (unter anderem in das Netzwerk) eingreift. Selbstverständlich muss das Betriebssystem regelmäßig auf Schwachstellen geprüft werden, und Patches zeitnah eingespielt werden.

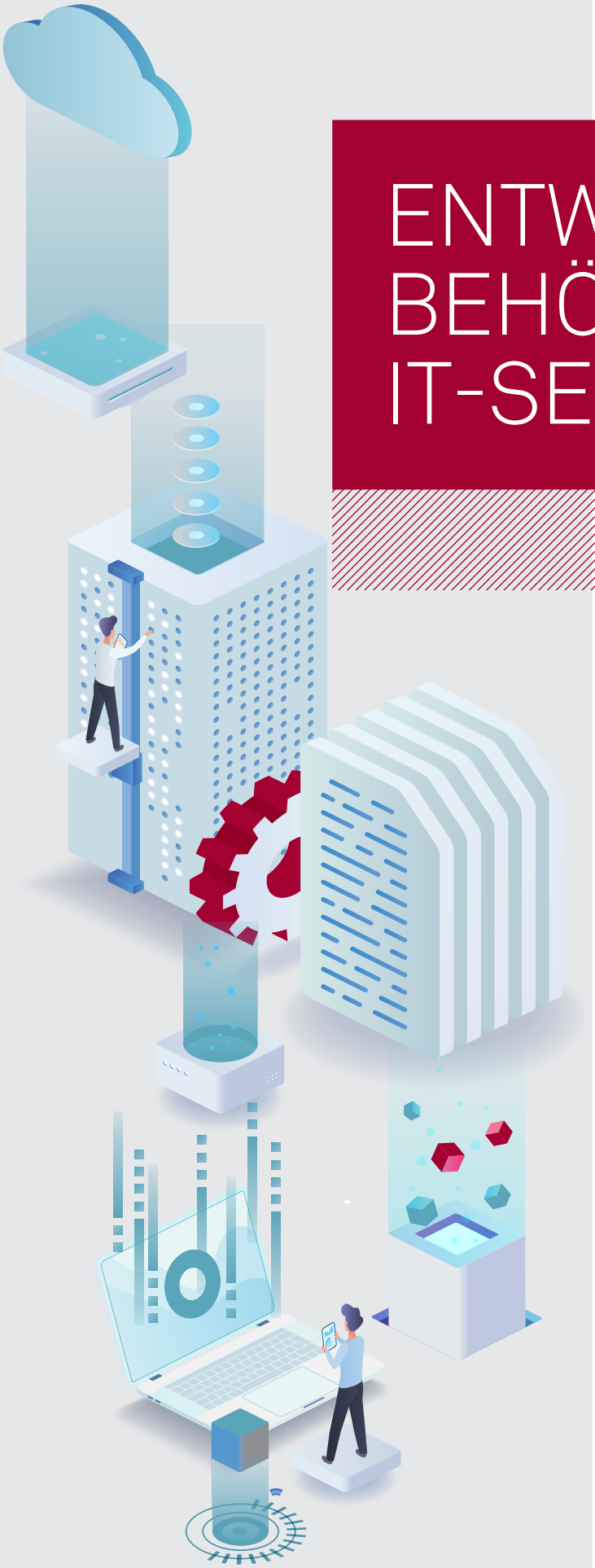
Die Container zu von außen erreichbaren Services sollten in Kubernetes dedizierten Rechnern (Ingress-Knoten) zugewiesen werden. Dieses Pinning erlaubt eine bessere Trennung der Container, auch kann man anhand der IP-Adressen beispielsweise den Zugriff auf Persistent-Volumes knotenfremder Container oder auf die externen Datenbanken unterbinden. Ein Angreifer, der einen von außen erreichbaren Container oder einen Container eines anderen Verfahrens und anschließend den Knoten übernommen hat, kann so nicht auf die Datenablage der internen Container zugreifen. So lässt sich auch eine Drei-Schichten-Architektur realisieren. Alternativen sind, für beide Bereiche verschiedene Cluster mit getrennten Orchestratoren aufzubauen oder die erste Schicht auf separaten Rechnern ohne Orchestrator aufzubauen. Beim Mehrmandantenbetrieb auf dem Cluster kann man mit Pinning für eine bessere Trennung etwa die Knoten den Containern der Anwendungen dediziert zuordnen.

Zwischen den Knoten sollten keine Zugriffe (vor allem nicht über SSH) möglich sein, sondern nur über einen abgesetzten Admin-Rechner als Bastion-Host. So kann ein Angreifer, der einen Knoten infiltriert hat, diesen nicht als Sprungbrett auf andere Knoten des Clusters nutzen (Server Hopping).

AUSBLICK

Die Container-Technologie verändert die Entwicklung und den Betrieb von Anwendungen nachhaltig. Manche der bekannten Sicherheitsmaßnahmen gelten unverändert, andere müssen an die neuen Gegebenheiten angepasst werden. Dies trifft gleichermaßen auf die Sicherheitswerkzeuge zu, die oft noch nicht für die Container-Technologie ausgelegt sind. Die leistungsstarken Tools von Start-ups wie „AquaSec“[12], „Neuvector“[13] oder „Twistlock“[14] zeigen den Weg: Sie setzen stärker auf Verhaltensanalysen und Automatisierung. Die Werkzeuge frieren beispielsweise Container mit verdächtigtem Verhalten ein und starten automatisch einen neuen Container mittels des ursprünglichen Images. ●

1 https://jaxenter.de/zuul-2-gateway-plattform-open-source-71405 (abgerufen am 06.07.2020).
2 Wolff, Eberhard: „Microservices – Ein Überblick“, innoQ Deutschland GmbH, 2018.
3 vgl. .public Ausgabe 01-2020, Tim Pommerening: „Betreutes Wohnen für Altanwendungen“.
4 NIST-Standard SP 800-180.
5 https://kubernetes.io/de/docs/tutorials/kubernetes-basics/ (abgerufen am 06.07.2020).
6 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5736 (abgerufen am 06.07.2020).
7 National Institute of Standards and Technology (NIST): „Application Container Security Guide“, Special Publication 800-190, 2017.
8 Center for Internet Security: „CIS Docker 1.13.0 Benchmark“, v1.0, 2017; Center for Internet Security: „CIS Kubernetes Benchmark“, v1.5.1, 2020.
9 https://www.sonarqube.org/ (abgerufen am 06.07.2020).
10 Ein Service-Mesh ist eine Infrastrukturebene für die sichere und zuverlässige Kommunikation zwischen den Diensten einer Anwendung, die auf dem Netzwerk aufsetzt.
11 NCC Group: „Understanding and Hardening Linux Containers“, Whitepaper, 2019.
12 https://www.aquasec.com/solutions/kubernetes-container-security/ (abgerufen am 06.07.2020).
13 https://neuvector.com/kubernetes-security-solutions/ (abgerufen am 06.07.2020).
14 https://www.twistlock.com/dockerfederalsummit/22/ (abgerufen am 06.07.2020).



ENTWICKLUNG BEHÖRDLICHER IT-SERVICES

Cloud in Behörden, Teil 5

| von LUDWIG SCHERR

In den letzten Beiträgen zu Cloud- und IT-Service-Management wurden – zum Teil behördenspezifische – Merkmale einer Cloud-Organisation behandelt. In diesem Beitrag geht es um die Vorgehensweise zur Entwicklung von IT-Services, für die es im behördlichen Umfeld keine grundsätzlichen Unterschiede zu kommerziellen IT-Service-Providern gibt. Vielmehr spielen IT-Service-spezifische Domänen eine Rolle, die sich von denen der Softwareentwicklung doch wesentlich unterscheiden.

Aus der Softwareentwicklung sind klassische Vorgehensmodelle wie Wasserfallmodell oder Spiralmodell bekannt, die durch agile Methoden wie Scrum oder Kanban ergänzt oder abgelöst werden. Klassischen und agilen Vorgehensweisen ist gemeinsam, dass am Anfang Anforderungen stehen, die die Basis für den Systementwurf bilden. Die Implementierung folgt dann dem Systementwurf und das Testen prüft, ob die Anforderungen in der notwendigen Qualität umgesetzt wurden.

Und wie sieht es nun bei den IT-Services aus? Im Grunde genommen gibt es in der Vorgehensweise keine Unterschiede zur Softwareentwicklung. Es müssen Anforderungen vorliegen, auf deren Basis ein Entwurf erstellt wird. Dieser wird umgesetzt und in einem Test der Qualitätskontrolle unterzogen. Der Unterschied liegt in den IT-Service-spezifischen Domänen.

Ein IT-Service ist wie folgt definiert: Ein vom Software-Provider bereitgestelltes Softwareprodukt wird zu einem nutzbaren Service weiterentwickelt, sodass aus einer zu installierenden Software ein vom Kunden direkt nutzbarer IT-Service entsteht. Auf diese Weise unterstützt der IT-Service die Geschäftsprozesse der Behörde „direkter". Bei einer Behördenanwendung heißt das beispielsweise, dass das installierbare Softwarepaket des Software-Providers mit unterstützenden IT-Services – zum Beispiel virtuelle Server mit Netzanbindung und Storage, Datenbank, Applikationsserver, Loadbalancer etc. – zu einem kundengerichteten IT-Service gebündelt wird. Für einen vollständigen kundengerichteten IT-Service, der als Up-and-running-IT-Service zur aktiven Nutzung den Anwendern des Kunden bereitgestellt werden kann, müssen die IT-Service-spezifischen Domänen noch integriert werden. Auch in den IT-Service-spezifischen Domänen, wie User Help Desk, Incident-Management, Capacity-Management oder Service-Level-Management, müssen, analog der Softwareentwicklung, Design- und Build-Aktivitäten durchgeführt werden, um die neue Behördenanwendung zu einem vollständigen IT-Service zu machen.

Der Kern dieses Artikels beschäftigt sich mit den Schritten, die aus einem installierbaren Softwarepaket einen nutzbaren IT-Service mit definierten Service-Leveln machen.

Wie oben beschrieben stehen am Anfang eines IT-Services die Anforderungen – in diesem Fall die betrieblichen Anforderungen (Service-Level-Requirements), die der zu entwickelnde IT-Service erfüllen muss. In der Regel sind die Service-Level-Klassen, in die der neu zu erstellende IT-Service eingruppiert werden soll, bereits definiert.

Idealerweise wurde dieser neue IT-Service bereits im Vorfeld in das Portfoliomanagement für IT-Services eingebettet. Auch die Grundinformationen zum neuen IT-Service liegen seit Längerem vor, sodass eine ausgiebige Planung bereits im Vorfeld vor Übergabe des Software-Packages möglich war. Zu diesen Grundinformationen zählen, neben der Grobbeschreibung des IT-Services, Merkmale wie Anzahl Nutzer/Zeiteinheit, notwendige unterstützende IT-Services, Service-Level-Anforderungen des Kunden, geschätzter Realisierungsaufwand und ungefähre Realisierungsdauer etc. Im Service-Design und in der Realisierung des IT-Services gibt es drei Ebenen, die zu betrachten sind.

1. Die Sicht auf die **technische Komponentenebene**, die IT-Operations, den „Maschinenraum", betrifft. In dieser Ebene wird der IT-Service aus technischer Sicht erbracht und gesteuert. Hier liegen beispielsweise die Ressourcen-Pools für die Service-Instanziierung oder das Monitoring für die Komponentenüberwachung.

DEFINITE MEDIA LIBRARY (DML)

Bereich zur sicheren Speicherung von Softwarepaketen und zugehörigen Artefakten wie Dokumenten. Die DML ist Bestandteil des Configuration-Management-Systems.

SERVICE-KATALOG

Der Service-Katalog enthält Informationen zu allen verfügbaren und im Deployment befindlichen IT-Services. Kundengerichtete IT-Services sind im Bestellportal sichtbar, unterstützende IT-Services sind in kundengerichteten IT-Services integriert. Die im Service-Katalog hinterlegte Leistungsbeschreibung zu einem IT-Service informiert über den Leistungsumfang.

SERVICE-INVENTAR

Das Service-Inventar enthält alle instanziierten IT-Services mit den zugrunde liegenden Unterlagen wie Bestellungen, Verträge oder Service-Level-Agreements. Die IT-Service-Instanzen sind mit den technischen Services/Komponenten in CMDB verknüpft.

CMDB, CI UND CI-MODELL

Die CMDB (Configuration-Management-Database) ist der Speicherort für CIs (Configuration-Items), die auf Komponentenebene die technischen Services und Komponenten identifizieren. CIs sind in einem CI-Modell eingebunden, das die Struktur und Vernetzung verschiedener CIs insgesamt darstellt.

IT-SERVICE-SPEZIFISCHE DOMÄNEN

Gegenüber der Softwareentwicklung sind in der Entwicklung eines IT-Services andere Fachbereiche relevant. Das gelieferte Softwarepaket muss beispielsweise in das Configuration-Management, das Availability-Managment oder das Incident- und Problem-Management eingebettet werden. In der Softwareentwicklung stehen beispielsweise Software-Design und Schnittstellen im Vordergrund.

2. Die **Service-Ebene**, in der die technischen Komponenten zu einem IT-Service aggregiert und als solcher ganzheitlich gemanagt werden. Dies betrifft beispielsweise das Service-Inventar, in dem alle Service-Instanzen geführt werden.
3. Die **Business-Ebene**, in der die Aspekte des Kunden und der IT-Service-Provider-Strategie betrachtet werden. Hier werden alle IT-Services eines Kunden aggregiert betrachtet. Sowohl die IT-Service-Verrechnung als auch das IT-Service-Portfoliomanagement sind hier angesiedelt.

Abbildung 1: Komponenten-Ebene in der IT-Serviceentwicklung

(siehe in diesem Zusammenhang auch den Artikel „Automatisierte Bereitstellung von IT-Services“, .public 02-2019) .Im Folgenden werden diese drei Ebenen näher betrachtet, und dabei wird auf die wichtigsten Inhalte eingegangen.

TECHNISCHE KOMPONENTENEBENE (IT-OPERATIONS)

- Vom Software-Provider wird das Softwarepaket der Behördenapplikation mit der begleitenden Dokumentation bereitgestellt. Darin sind die Applikationsstruktur sowie die notwendigen Plattform- und Infrastrukturservices beschrieben, die die Grundlage für die einzelnen Komponenten der Behördenapplikation darstellen. So wird beispielsweise beschrieben, wie das Frontend der Behördenapplikation auf einen definierten Applikationsserver und das Backend auf eine definierte Datenbank aufgebracht wird. Das übergebene Softwarepaket wird mit allen Bestandteilen inklusive Dokumenten in das zentrale Repository für Software-Packages der Behördenapplikationen, der „Definitive Media Library“ (DML), eingebracht.
- Im Rahmen des Configuration-Managements wird für den neuen IT-Service ein Configuration-Item-Modell (CI-Modell) erzeugt, das die technische Sicht auf die einzelnen Configuration Items (CIs) im vernetzten Zusammenhang darstellt. Das CI-Modell findet Eingang in die Configuration-Management-Datenbank (CMDB), in der es als Modell hinterlegt wird.
- Für die Bereitstellung der einzelnen Applikationskomponenten und der darunterliegenden Plattform- und Infrastruktur-IT-Services werden Installations- und Konfigurationsskripte sowie -templates für die Produktionsstraße erstellt und als technische Blaupause für eine Instanziierung im Automatisierungsrepository hinterlegt. Hierdurch ist es möglich, die einzelnen Komponenten beziehungsweise Sub-Services automatisiert immer in gleicher Qualität und in verschiedenen Umgebungen bereitzustellen.
- Der neue IT-Service wird in die Überwachung (Monitoring) auf Komponentenebene integriert. Dies betrifft einerseits die Überwachung und andererseits die Messung:
  - Im Rahmen der Überwachung werden komponentenspezifische Alarme (Alerts) definiert und für eine Erzeugung von Komponenten-Tickets mit den in der CMDB hinterlegten CIs verknüpft.
  - Für die Messung werden Prozesskennzahlen- und SLA-Nachweis-relevante Prozeduren erstellt, so dass definierte Auswertungen und SLA-Nachweise im Betrieb generiert werden können. Dies betrifft auch den Aspekt der Verbrauchserfassung zur Messung der Verbräuche auf Basis des Service-Designs. Die Verbrauchsmengen werden an die Serviceebene kommuniziert.
- Die für den neuen kundengerichteten IT-Service eingerichteten Überwachungen und Messungen werden in die bestehenden Standardberichte auf Komponentenebene integriert.

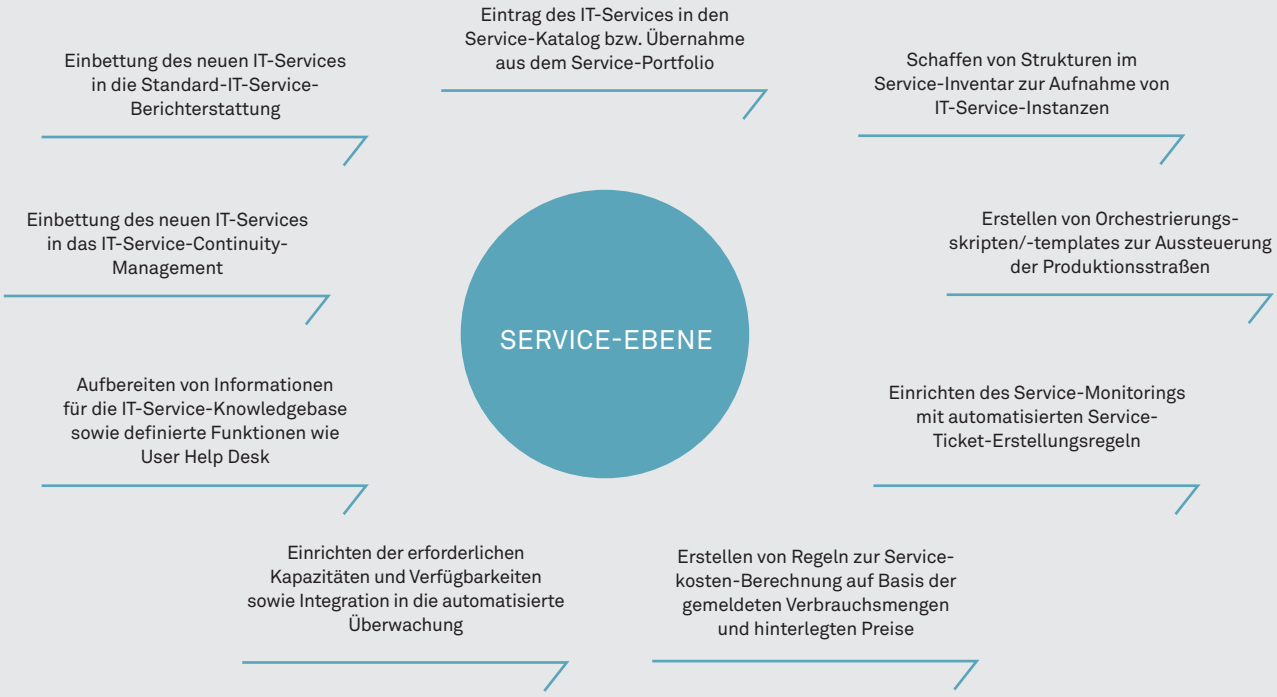


Abbildung 2: Service-Ebene in der IT-Service-Entwicklung

SERVICE-EBENE

- Im Service-Katalog werden die Eintragungen für den freizuschaltenden Service aus der Service-Pipeline übernommen und um aktuelle Informationen, wie Leistungsbeschreibung und Servicebaum, ergänzt. Der Service-Katalog enthält somit alle notwendigen Informationen, die den IT-Service beschreiben.
- Im Service-Inventar werden Vorbereitungen getroffen, so dass nach einer erfolgreichen Service-Orchestrierung die Service-Instanzen mit Verlinkungen in die CMDB der technischen Service-Ebene eingetragen werden können.
- In der Service-Orchestrierung werden Skripte zur Aussteuerung der Service-Instanziierung auf Komponentenebene in den einzelnen Produktionsstraßen erstellt. Die beteiligten „Komponenten-Services" sind aus dem Servicebaum des Service-Katalogs zu entnehmen. Instanziierte Services der Service-Ebene werden im Service-Inventar eingetragen.
- Das Service-Monitoring wird eingerichtet und mit dem Monitoring auf Komponentenebene verknüpft. So wird auf Basis von Komponenten-Alerts entschieden, wann ein Alert auf IT-Service-Ebene ausgelöst wird. Aufgrund eines IT-Service-Alerts kann ein Serviceticket eingestellt werden.
- Die Verbrauchsmengen aus der Komponentenebene werden hier zu Servicekosten ausgewertet und akkumuliert.
- Die erforderlichen Kapazitäten für die IT-Services werden aus den Service-Level-Anforderungen sowie aus dem prognostizierten Nutzungsvolumina ermittelt, im Kapazitätsplan hinterlegt und an die technische Ebene zur Berechnung der erforderlichen Zahl an IT-Service-Instanzen weitergeleitet. Die Auslastung und Performance von IT-Services wird verfolgt.
- Die erforderlichen Verfügbarkeiten werden ebenfalls aus den Service-Level-Anforderungen abgeleitet und mit der technischen Ebene abgestimmt. Die erforderlichen Kennzahlen werden in das Monitoring integriert, um einerseits dem Kunden die IT-Service-Verfügbarkeit nachweisen zu können und andererseits Hinweise für Optimierungsmaßnahmen ableiten zu können.
- Für den Service-Desk werden entsprechende Informationen wie Checklisten oder Lösungsbäume zur Behandlung oder Eingrenzung von auftretenden Störungen erstellt.
- Im IT-Service-Continuity-Management werden die in einem Katastrophenfall mindestens erforderlichen Service-Level betrachtet, und der aktuelle Service wird darin eingebettet.
- Letztendlich wird im Service-Reporting der neue IT-Service eingebunden, und die Berichte werden entsprechend erweitert beziehungsweise ergänzt.

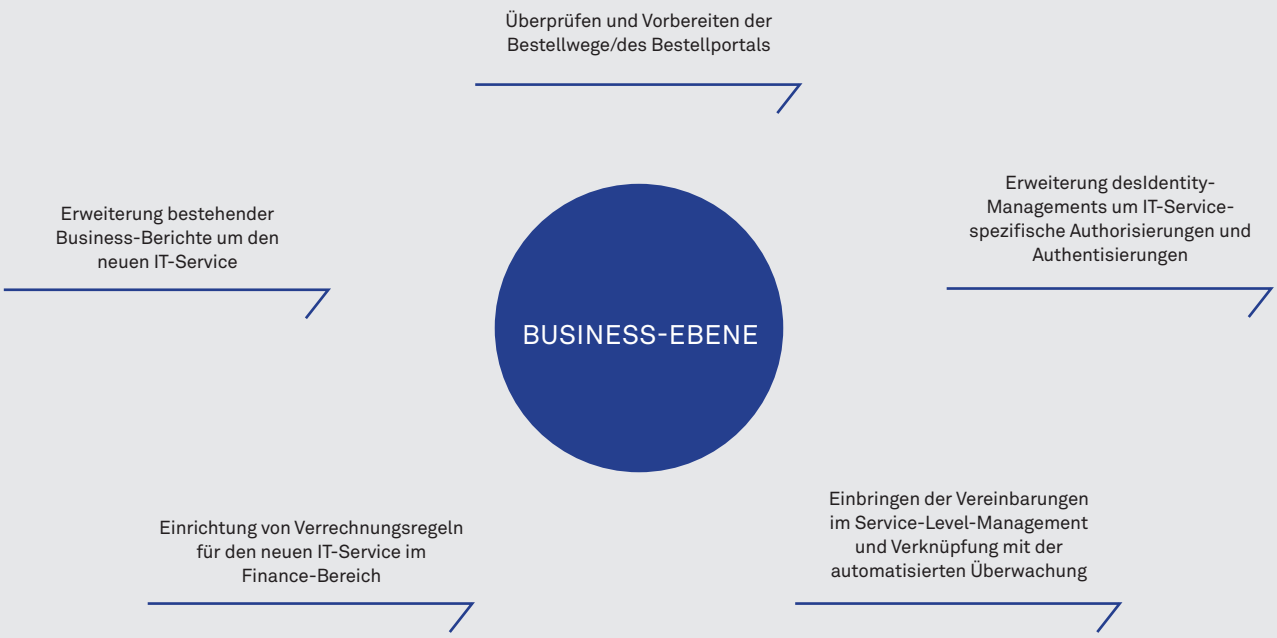


Abbildung 3: Business-Ebene in der IT-Serviceentwicklung

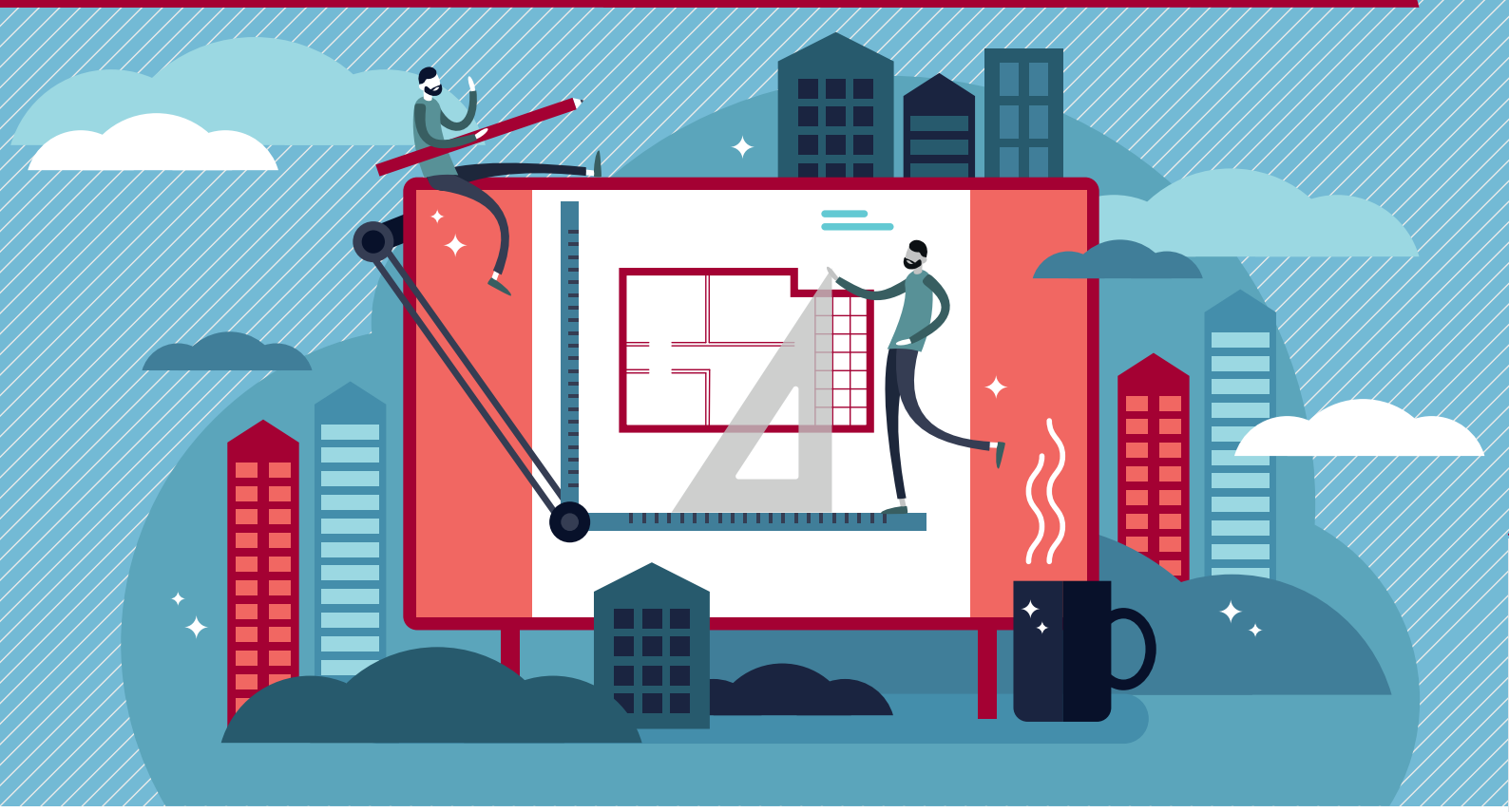
BUSINESS-EBENE

- Wenn die Schnittstellen vom Service-Katalog und zur Service-Orchestrierung so weit offen sind, dass die service-spezifischen Informationen als Variablen abgebildet sind, sind im Idealfall in den etablierten Bestellkanälen keine Anpassungen notwendig.
- Im Identity-Management muss der neue IT-Service eingebettet werden, so dass die Bestellberechtigung sowie die Kundenzuordnung ausgesteuert werden kann. Authentifizierungen und Autorisierungen werden eingerichtet.
- Die mit dem Kunden vereinbarten Service-Level müssen in eine neue beziehungsweise in bereits bestehende Vereinbarungen eingebettet werden. Für die Operational Level Agreements der unterstützenden IT-Services wird überprüft, ob diese die zugesicherten Servicewerte wie Verfügbarkeit und Performance unterstützen. Die vereinbarten Service-Level werden dem Monitoring mitgeteilt, so dass dort die Skripte für die Messung der Kennzahlen erstellt werden können.
- Im Finance-Bereich werden Service-Instanzen des neuen IT-Services kundenbezogen akkumuliert und für den Kostennachweis und die Kostenverrechnung verwendet.

ZUSAMMENFASSUNG

Diese Aktivitäten im Rahmen der Erstellung eines IT-Services stellen nur einen groben Überblick über die notwendigen Schritte zur Entwicklung eines vom Anwender nutzbaren IT-Services dar. Aber es ist erkennbar, dass sich die Entwicklung eines IT-Services doch deutlich von der Entwicklung einer Anwendungssoftware unterscheidet. ●

WIRKUNGSVOLLE ARCHITEKTURDOKUMENTATION ALS ERFOLGSFAKTOR (NICHT NUR) FÜR AGILE PROJEKTE



| von DR. ATILA KAYA

Beim Thema Architekturdokumentation stellt sich in Softwareprojekten immer wieder eine Reihe von typischen Fragen: Wie und von wem soll die Architektur dokumentiert werden? Wie kann Architekturdokumentation in die Teamarbeit integriert werden und sie unterstützen, um eine qualitativ hochwertige Softwarelösung zu liefern? Wie können Architekturentscheidungen in der Praxis transparent und nachvollziehbar an die Stakeholder werden, und wie kann der Weg für zukünftige Architekturreviews geebnet werden?

ARCHITEKTURENTSCHEIDUNGEN

In der Praxis haben sich Wikis als Werkzeug für die Erstellung sowie die Ablage von Architekturentscheidungen bewährt. Sie bieten gleich mehrere Vorteile: Wiki-Software fördert Transparenz und Kollaboration und bietet komfortable Such- und Verlinkungsmöglichkeiten. Richtig eingesetzt, zum Beispiel durch die Nutzung von Kommentar- und Benachrichtigungsfunktionen, kann Wiki-Software Architekturmanagementprozesse, wie beispielsweise Gremienarbeit, unterstützen.

Eine potenzielle Schwäche bei der Nutzung von Wikis zur Architekturdokumentation ist die unzureichende Unterstützung für die Erstellung und Bearbeitung von Abbildungen und Tabellen. Daher sollte bei der Auswahl der Wiki-Software besonderes Augenmerk auf diese Punkte gelegt werden. Gute Produkte wie Confluence[3] oder MediaWiki[4] ermöglichen effiziente Erstellung, Bearbeitung und Versionierung von Abbildungen innerhalb des Wikis, zum Beispiel durch sogenannte Plug-ins.

Eine weitere Schwäche von Wikis sind die Exportmöglichkeiten für die Inhalte – wenn zum Beispiel der Inhalt oder ein Teil dessen als eine PDF-Datei mit Inhaltsverzeichnis und entsprechendem Layout für den Druck exportiert werden soll. Abhängig vom Produkt und von den Anforderungen an das Layout des exportierten Dokuments können hier größere Aufwände entstehen.

Die vielleicht größte Schwäche von Wikis für die Architekturdokumentation ist die Versionierung von Inhalten, die zwar von Wiki-Software übernommen wird, allerdings unabhängig von der Versionierung der Software ist. Möchte man Software und Architekturdokumentation gemeinsam versionieren, muss in der Regel mit umständlichen Behelfslösungen gearbeitet werden. Die Ursache dieses Problems ist die fehlende Nähe und Verknüpfung von Dokumentation und Quellcode. Darauf gehen wir im weiteren Verlauf dieses Artikels ein und stellen eine Lösung vor.

Nicht selten herrscht in Projektteams keine klare Vorstellung über Form, Gliederung und Inhalt der notwendigen Dokumentation. Gute Vorlagen für Dokumentationen sind daher sehr wertvoll. Dabei hat sich folgende Struktur als Vorlage für Architekturentscheidungen in der Praxis bewährt (siehe Tabelle nächste Seite):

Software-Architektur, Software-Architekt, Architekturentscheidungen und Architekturarbeit

Nach Martin Fowler besteht Software-Architektur aus Softwaredesign-Entscheidungen, die sowohl wichtig als auch schwer zu ändern sind – eine Definition, der wir uns anschließen. Wie auch Stefan Zöller nennen wir diese Art von Entscheidungen „Architekturentscheidungen“.[1]

Unter Architekturarbeit, also dem Erarbeiten der Architektur, verstehen wir zum einen das Entwerfen der Lösung. Zum anderen auch die nachvollziehbare Herleitung von Architekturentscheidungen sowie die Verantwortung für deren Umsetzung. Laut ISAQB, dem International Software Architecture Qualification Board, das sich die Lehre, Aus- und Weiterbildung für Software-Architektur auf die Fahne geschrieben hat, sind die sechs Kernaufgaben der Architekturarbeit wie folgt (siehe Abbildung 1):[2]

Ein Softwarearchitekt ist derjenige, der die Architekturarbeit ausführt, unabhängig vom Projektvorgehen (klassisch oder agil) und vom Rollenverständnis (expliziter Architekt oder nicht).

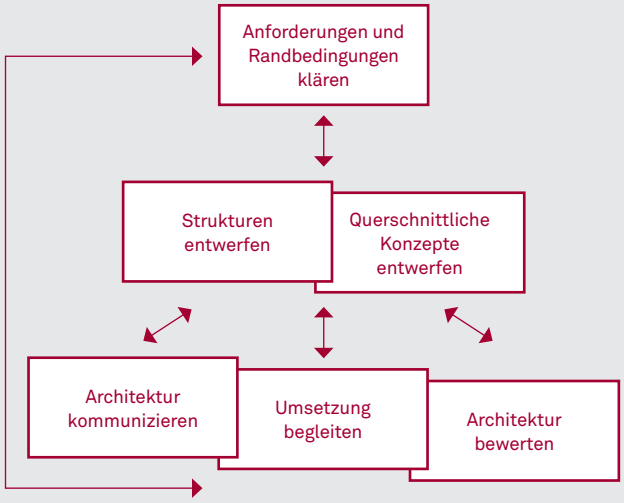


Abbildung 1: Sechs Kernaufgaben der Architekturarbeit

ABSCHNITT	BESCHREIBUNG
Fragestellung	Problembeschreibung, Relevanz für die Architektur
Einflussfaktoren	Randbedingungen, Qualitätsziele, betroffene Risiken
Annahmen	Getroffene Annahmen, neue Risiken
Alternativen	Beschreibung der Lösungsoptionen, ausgeklammerte Lösungsoptionen
Kriterien	Feste Kriterien, zusätzliche Kriterien
Entscheidung und Begründung	Tabellarische Bewertung der Alternativen im Hinblick auf Kriterien, Zusammenfassung der Entscheidung mit kurzer Begründung
Auswirkungen	Nennenswerte Auswirkungen auf andere Entscheidungen und auf die Strategie
Zugehörige Entscheidungen	Weitere Entscheidungen, die im Zusammenhang stehen

Tabelle 1: Vorlage für Architekturentscheidungen

Feste Kriterien haben sich in mehreren Projekten als sehr nützlich erwiesen (siehe Abbildung 2). Bei Bedarf kann für jede Architekturentscheidung die Liste um zusätzliche Kriterien erweitert werden.

ARCHITEKTURÜBERBLICK

Für die Dokumentation der Architektur eines Softwaresystems stellt arc42.org ein erprobtes Template in verschiedenen Formaten unter der Lizenz Creative Commons Attribution zur Verfügung.[5]

Danach wird eine kompakte Architekturdokumentation wie folgt gegliedert (siehe Tabelle 2).

Qualitätsmerkmale sind Anforderungen an das Softwaresystem, die über die etwa in User-Storys beschriebenen fachlichen Funktionalitäten hinausgehen, wie zum Beispiel „Zuverlässigkeit“ oder „Wartbarkeit“. Für die Prüfung von Qualitätsmerkmalen sollte die Prüfung der Einhaltung von Architekturvorgaben im Idealfall automatisiert und kontinuierlich stattfinden. Hierfür stehen mit jQAssistant[6] und Neo4J[7] Open-Source-Werkzeuge zur Verfügung, die sich mit überschaubarem Aufwand in

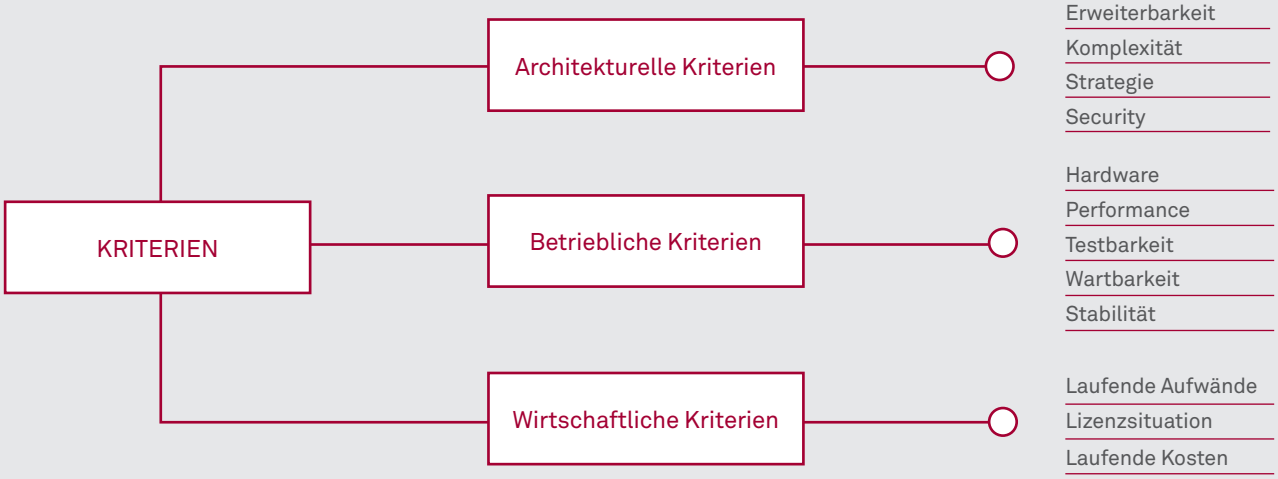


Abbildung 2: Beispielkriterien für Architekturentscheidungen

KAPITEL	BESCHREIBUNG
Einführung und Ziele	Aufgabenstellung, Qualitätsziele, Stakeholder
Randbedingungen	Wichtigste Vorgaben, die einzuhalten sind
Kontextabgrenzung	Fachlicher Kontext, technischer Kontext
Lösungsstrategie	Architekturziele mit zugeordneten Architekturansätzen, Verweise auf Details der Lösung
Bausteinsicht	Statische Sicht auf die Systemstruktur: Whitebox-Gesamtsystem, Ebene 2 und Ebene 3
Laufzeitsicht	Das Verhalten des Systems zur Laufzeit: Ablaufdiagramme für die wichtigsten Aspekte des Systems
Verteilungssicht	Verteilung des Systems: Beschreibung der Laufzeitumgebung, Zuordnung von Bausteinen zu Deployment Units, Zuordnung der Deployment Units auf die Zielumgebung
Querschnittliche Konzepte	Technische, übergreifende Konzepte wie zum Beispiel Persistenz, Caching oder Fehlerbehandlung
Entwurfsentscheidungen	Architekturentscheidungen
Qualitätsanforderungen	Präzisierung von Qualitätsmerkmalen in konkreten Szenarien, Zuordnung der Szenarien zu Merkmalen in einem Qualitätsbaum
Risiken und technische Schulden	Risiken, die die Architekturentscheidungen beeinflusst haben. Bewusst oder unbeabsichtigt eingegangene Qualitätskompromisse
Glossar	Klärung wichtiger Begriffe zur Etablierung eines gemeinsamen Wortschatzes im Projekt

Tabelle 2: für kompakte Architekturdokumentationen

Continuous Integration(CI) Pipelines integrieren lassen. Die Ergebnisse der Prüfung von Architekturvorgaben können dann mithilfe von Plug-ins in SonarQube[8] integriert werden.[9] Diese Integration ermöglicht die gemeinsame Betrachtung von Ergebnissen der statischen Codeanalyse und die Prüfung von weiteren Qualitätsmerkmalen in der SonarQube-Plattform.

ARCHITEKTURPRÄSENTATION

Die nachfolgend skizzierte Situation ist typisch für den Projektalltag: Neue Projektmitglieder oder andere Stakeholder wollen sich einen schnellen Überblick über das Projekt sowie die Lösungsansätze verschaffen. Allerdings finden sie entweder keine Informationen oder aber sehr detaillierte Informationen. Ein Überblick über Projektziele, Herausforderungen und Lösungsansätze auf einer konzeptionellen Ebene fehlt.

Dabei ist die zielgerichtete Kommunikation der Architektur mit geeigneten Mitteln ein wichtiger Faktor für den Projekterfolg. Ein aktueller aus zehn bis fünfzehn Folien bestehender Foliensatz ist eine wertvolle Unterstützung zur Präsentation der Problemstellung und der zentralen Lösungsansätze. Die Architekturpräsentation hat das Ziel, die Informationen aus dem Architekturüberblick in kompakter Form zu wiederzugeben. Hier hat sich folgende Struktur für die Architekturpräsentation in der Praxis bewährt (siehe Tabelle 3):

ABSCHNITT	INHALTE
Problemstellung	Fachlicher Überblick, Ziele, Kontext, Randbedingungen
Lösungsstrategie	Architekturprinzipien, eingesetzte Produkte und Technologien
Details der Lösung	Struktur, Verhalten und Verteilung des Systems
Ausblick	Nächste Schritte, weiterführende Informationen

Tabelle 3: Vorlage für die Strukturierung von Architekturpräsentationen

DOCS-AS-CODE

In den letzten Jahren entstand für die Erstellung der Dokumentation ein neuer Ansatz mit dem Ziel, die fehlende Nähe zwischen Dokumentation und Quellcode durch gut geeignete Werkzeuge herzustellen und dadurch die Motivation von Entwicklungsteams bei der Erstellung und Pflege der Dokumentation zu erhöhen. Für diesen Ansatz hat sich der Begriff „Docs-as-Code" etabliert.[10] Hier wird die Dokumentation in AsciiDoc, einem rein textbasierten Format mit einfacher Syntax, erstellt, analog zu Quellcode in einem Repository verwaltet sowie in den Build- und Testprozess der Software integriert. Die Verwaltung der Dokumentation in einem Repository, wie zum Beispiel git[11], ermöglicht die gleichen Workflows für die Dokumentation wie für den Quellcode: Versionierung, Reviews, Branching, Merging usw. Zudem kann mit dem Open-Source-Konverter AsciiDoctor[12] die in AsciiDoc erstellte Dokumentation in verschiedene Ausgabeformate wie HTML5, DOCX oder PDF konvertiert werden.

Das in Gradle[13] entwickelte Open-Source-Werkzeug docToolchain nutzt AsciiDoctor und Pandoc[14] als Konverter und treibt die Automatisierung der Dokumentenerstellung konsequent weiter.[15] Hierfür bringt docToolchain eine Reihe von Gradle-Modulen (Tasks) mit, die bei Bedarf auch erweitert werden können. Mit docToolchain können zum Beispiel Diagramme aus Sparx Enterprise Architect (EA)[16] oder Tabellen aus MS Excel durch entsprechende Tasks exportiert und in die auf arc42-Vorlage basierende Architekturdokumentation im AsciiDoc-Format eingebunden werden. Dabei unterstützt der Include-Task die Verteilung der Dokumentation auf mehrere Dateien und somit deren Modularisierung. Durch eine gut durchdachte Modularisierung der Dokumentation wird eine bessere Übersichtlichkeit erzielt, die Zusammenarbeit im Team verbessert, und Teile der Dokumentation in verschiedenen Kontexten werden wiederverwendbar gemacht. Darüber hinaus bietet docToolchain weitere Tasks, um die Dokumentation automatisch nach Problemen wie fehlerhaften Links oder fehlenden Bildern zu prüfen.

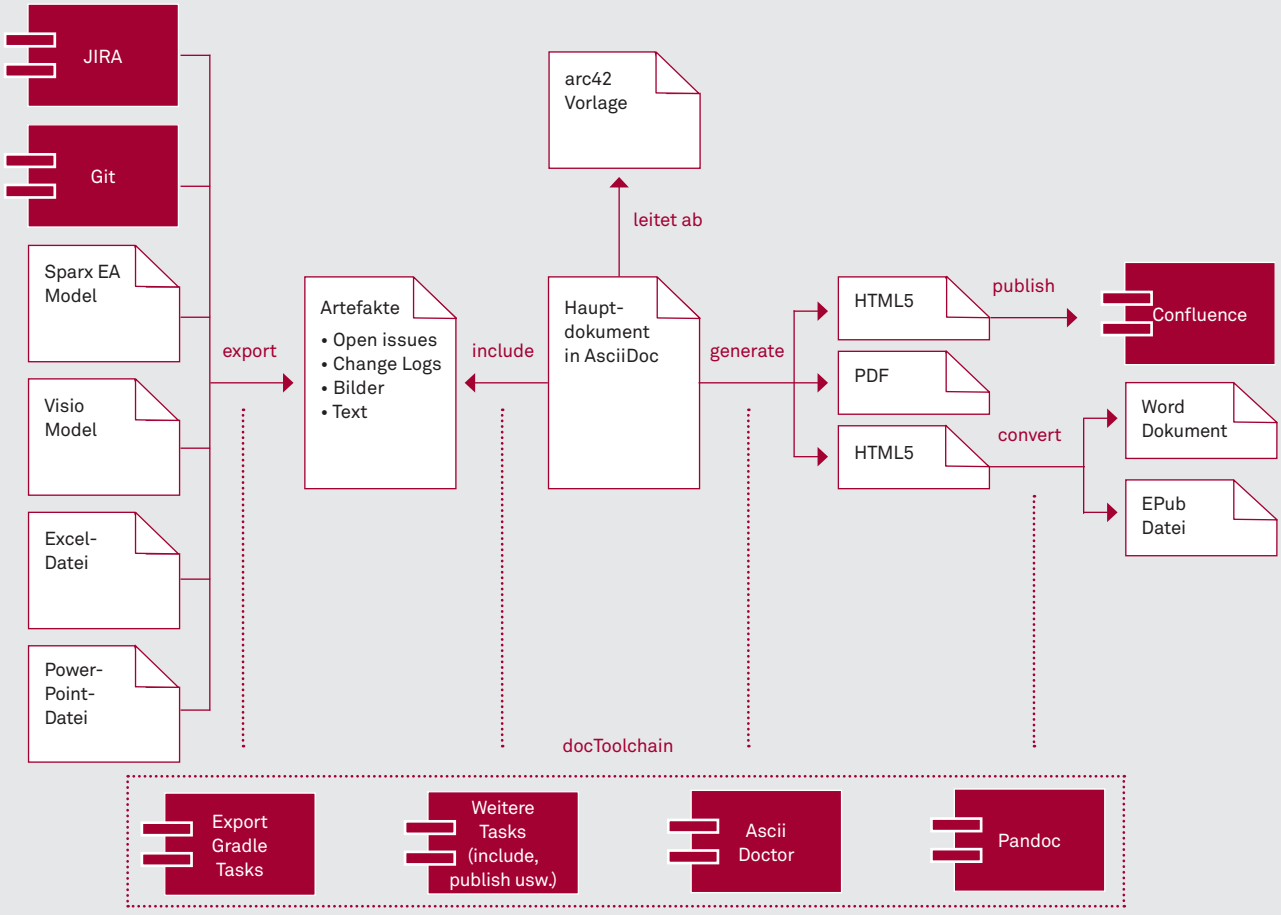


Abbildung 3: Übersicht der Dokumentenerstellung mit docToolchain

Am Ende der Werkzeugkette wird die Architekturdokumentation im gewünschten Ausgabeformat, wie zum Beispiel als PDF- oder Word-Dokument, generiert. Alternativ kann die Dokumentation in Wiki-Syntax generiert und in Confluence publiziert werden.

Wenn die Dokumentation dem Docs-as-Code-Ansatz folgend im AsciiDoc-Format erstellt und im gewünschten Ausgabeformat generiert wird, dann muss sie auch in AsciiDoc weiter gepflegt werden. Demzufolge profitiert man zwar bei einer generierten Confluence-Seite von Confluence-Features wie zum Beispiel „Suchen", „Seite beobachten" oder „Kommentieren", darf aber die generierte Seite nicht in Confluence editieren.

Mit docToolchain können auch Word-Dokumente in AsciiDoc konvertiert und in den Build-Prozess integriert werden. Deshalb kann es auch in Projekten eingesetzt werden, in denen einige Stakeholder weiterhin mit Word arbeiten. Allerdings hat die automatische Konvertierung von DOCX in AsciiDoc ihre Grenzen, so dass einige formale Vorgaben bei der Erstellung des Word-Dokuments eingehalten werden müssen, um manuelle Schritte vor der Konvertierung zu vermeiden.

Es stellt sich insbesondere für die Architekturdokumentation die Frage, welche Aspekte der Dokumentation besser nah am Quellcode dokumentiert werden sollten. Es empfiehlt sich, diese Entscheidung im Hinblick auf organisatorische und projektspezifische Bedingungen zu treffen und die Dokumentation entsprechend zu modularisieren. Zum Beispiel kann ein Detailkonzept zur Replikation von Datenbankclustern, das von einer anderen Organisationseinheit oder einer externen Firma als Word-Dokument geliefert wird, nach der Konvertierung in die Architekturdokumentation im AsciiDoc-Format eingebunden werden, um am Ende Wiki-Seiten zu generieren und in Confluence zu publizieren.

FAZIT

Für die wirkungsvolle Gestaltung der Architekturdokumentation existieren erprobte Vorlagen, die die Form, Struktur sowie mögliche Inhalte vorgeben. Dadurch sinkt die Einstiegshürde für die Erstellung von qualitativ hochwertiger und wirksamer Architekturdokumentation. Die Inhalte müssen dabei zielgruppengerecht ausgesucht und je nach Anlass (zum Beispiel eine Präsentation oder ein Architekturüberblick) unterschiedlich detailliert und kombiniert werden.

Es empfiehlt sich insbesondere für agil umgesetzte Projekte, die Architekturdokumentation analog zum Quellcode iterativ und inkrementell zu erstellen. Mit dem Ziel, Aufwände zu reduzieren, kann die Erstellung und Pflege der Dokumentation, dem Docs-as-Code-Ansatz folgend, in den Test- und Releasezyklus der Software eingebunden werden. Für diesen immer populärer werdenden Ansatz existiert mit docToolchain ein ausgereiftes Open-Source-Werkzeug, das die kontinuierliche Erstellung und Pflege der Architekturdokumentation durch die Integration in den Build-Prozess unterstützt. Dadurch wird die Motivation, wirkungsvolle Architekturdokumentation auch ohne explizite Architekturrolle in Teamarbeit zu erstellen, deutlich verbessert. ●

1 Stefan Zöllner: Softwarearchitekturen dokumentieren und kommunizieren (2. Auflage). Carl Hanser Verlag 2015, Seite 18.
2 ISAQB: https://www.isaqb.org (abgerufen am 16.02.2020).
3 https://www.atlassian.com/de/software/confluence (abgerufen am 16.02.2020).
4 https://www.mediawiki.org/wiki/MediaWiki (abgerufen am 16.02.2020).
5 arc42: https://www.arc42.org/ (abgerufen am 16.02.2020).
6 https://jqassistant.org/ (abgerufen am 16.02.2020).
7 https://neo4j.com/ (abgerufen am 16.02.2020).
8 https://www.sonarqube.org/ (abgerufen am 16.02.2020).
10 https://www.writethedocs.org/guide/docs-as-code/ (abgerufen am 16.02.2020).
11 https://git-scm.com/ (abgerufen am 16.02.2020).
12 https://asciidoctor.org/ (abgerufen am 16.02.2020).
13 https://gradle.org/ (abgerufen am 16.02.2020).
14 https://pandoc.org/ (abgerufen am 16.02.2020).
15 https://github.com/docToolchain/docToolchain (abgerufen am 16.02.2020).
16 https://www.sparxsystems.de/ (abgerufen am 16.02.2020).

SCHULD IST (NICHT) CASSANDRA!

Kein Kassandraruf kann die wahren Helden schrecken, auch wenn sie wissen, sie wird Recht behalten.[1]

| von LASZLO LÜCK

Cassandra[2], als Vertreter moderner, verteilter Datenbank-Architekturen, findet in immer mehr Projekten Beachtung. Ein Grund ist, dass aktuelle IT-Architekturen zunehmend auf hochskalierbare und verteilte Architekturen aufbauen, da die zu verarbeitenden Datenmengen immer größer werden. Typische Anwendungsfälle finden sich in polizeilichen Vorgangsbearbeitungssystemen, Quasi-Echtzeit-Systemen zur Personenkontrolle und vor allem in großen Registeranwendungen, bei denen Cassandra als Big-Data-Speicher zum Einsatz kommt.

Cassandra wurde als ein Vertreter einer neuen Generation moderner Datenbank-Architekturen auf Konferenzen und in der Fachpresse vielfach beachtet. Dies führt dazu, dass bei der Projektplanung versucht wird, die Datenschicht „optimaler" gestalten zu können als mit traditionellen Datenbanken wie Oracle oder MySQL. Diesem anfänglichen Enthusiasmus folgte jedoch oftmals die Ernüchterung – verbunden mit dem Wunsch, doch wieder auf bewährte Technologien in Form von relationalen Datenbanken setzen zu können. Und das, obwohl die Ursachen für diese Ernüchterung in den meisten Fällen gar nicht bei Cassandra lagen, sondern daran, das auf Cassandra basierende System mit dem Wissen und der Erfahrung aus klassischen SQL-Datenbanksystemen betriebstechnisch zu unterhalten und softwareseitig zu benutzen. Der vorliegende Artikel zeigt die bisher gewonnenen Erfahrungen aus etlichen Projekten und reflektiert sie kritisch.

WOHER KOMMT CASSANDRA?

Cassandra ist ein Gemeinschaftsprojekt zweier Facebook-Mitarbeiter, die sich davon herausgefordert sahen, Informationen über eine sehr große Menge von Facebook-Nachrichten zu speichern, während die Nutzer gerade mit ihren Freunden im Facebook-Netzwerk kommunizierten.[3] Die zu erwartende Speichermenge und die vorgegebenen Randbedingungen des Betriebs seitens Facebook machten es erforderlich, ein völlig neues Datenspeicherkonzept zu entwickeln. Es sollte leicht skalierbar, aber kostengünstig sein. Das Ziel war, eine generische Datenbanklösung zu entwickeln, die für viele Anwendungszwecke verwendet werden kann.

Nach der Freigabe des Source Codes im Jahr 2008 steuerten weitere Unternehmen (IBM, Twitter, Netflix und viele mehr) Codes zu Cassandra bei. Im Jahr 2009 wurde das Projekt bei der Apache Software Foundation als Unterprojekt in den Apache Incubator aufgenommen. Im Februar 2010 wurde Cassandra von der Apache Software Foundation zum einem der sogenannten Top-Level-Projekte erklärt.

WAS IST CASSANDRA?

Cassandra ist ein extrem schnelles, skalierbares und ausfallsicheres Datenbanksystem, das sich hervorragend für die Speicherung sehr großer Datenmengen (1.8446744[19] Datensätze) eignet.

Ein Praxisbeispiel für die Resilienz und Ausfallsicherheit von Cassandra ist ein Vorfall aus dem Jahr 2014 bei der Firma Netflix: Durch das Einspielen eines Notfall-Security-Patches im Amazon-AWS-Stack mussten 218 der insgesamt über 2.700 Cassandra Nodes nahezu gleichzeitig neu gestartet werden. Nach der Wiederinbetriebnahme des betroffenen AWS-Netzes wurden alle Cassandra Nodes ohne Probleme wieder in die bestehende Landschaft integriert, ohne dass ein Kunde etwas vom Ausfall bemerkte.[4] Cassandra zeichnet sich außerdem als ein sehr schnelles Datenspeichersystem aus, sowohl beim Schreiben als auch Lesen von Daten.[5]

Sollten sich Engpässe beim Speicherplatz oder der Geschwindigkeit bemerkbar machen, ist es für einen IT-Betrieb mit entsprechendem Fachwissen sehr einfach möglich, weitere Cassandra Nodes dem Gesamtverbund (Node, Cluster – siehe Glossar) hinzuzufügen. Um die Neuverteilung der bereits im Cluster befindlichen Daten kümmert sich Cassandra automatisch. Sollten manuelle Eingriffe notwendig sein, bietet Cassandra hier Tools und Mechanismen, um Optimierungen zu ermöglichen. Dazu zählt beispielsweise die manuelle Verteilung der Daten oder Token auf den jeweiligen Nodes, wenn diese nicht mit dem gleichen Datenspeicherplatz ausgestattet sind.

Die Grenzen sind hier nur die Mauern des Rechenzentrums, in dem der Verbund betrieben wird. Aber selbst wenn das eine Rechenzentrum zu klein würde: Über Geo-Replikation ist Cassandra geradezu für den verteilten Einsatz über mehrere Standorte prädestiniert. Diese Eigenschaften machen Cassandra zu einem sehr ausfallsicheren Datenbanksystem.

Die Einfachheit beim Betrieb und die leichte Skalierbarkeit eines Cassandra-Clusters auf der einen Seite setzen fundierte Kenntnisse und Wissen als Softwarearchitekt und -entwickler auf der anderen Seite voraus. Der Ansatz des DevOps[6] (Developer und Operator) gewinnt beim Einsatz von Cassandra sehr große Bedeutung, denn nur mit dem technischen Wissen über Aufbau und Funktionsweise dieses Datenspeichers lässt sich Cassandra aus Sicht des Entwicklers korrekt nutzen.

WAS IST CASSANDRA NICHT?

Cassandra ist kein klassisches relationales Datenbanksystem (RDBMS). Weder erlaubt es die Speicherung und Ausführung von Geschäftslogik innerhalb der Datenbank (Stored-Procedures, Trigger) noch bietet es Relationen (Verbindungen/Beziehungen) zwischen Tabellen an. Außerdem ist Cassandra ein schemaloses Datenbanksystem (mittels eines Schemas legt man in einem klassischen RDBMS die Speichertechnik oder das Datenbankdesign fest).

Die fachliche Einordnung von Daten in Cassandra erfolgt mittels Keyspaces. Verfolgt man für die Modellierung der Software beispielsweise den Ansatz des Domain-Driven-Designs[7], kann man diesen bis in die Datenbank konsequent fortsetzen, da ein Keyspace für die Datenhaltung einer fachlichen Domäne verwendet wird. Technisch definiert man in einem Keyspace den Replikationsfaktor für die enthaltenen Daten.

Weniger gut ist Cassandra geeignet, wenn Datensätze häufig verändert werden. Ebenso erzeugt das häufige Löschen von Datensätzen eine höhere Last im Cassandra-Cluster, als man es von klassischen SQL-Servern gewohnt ist. Der Grund: Ein gelöschter Datensatz wird in Cassandra immer erst „zur Löschung markiert" und erst zu einem späteren Zeitpunkt aus dem Cluster physikalisch entfernt.

Ebenfalls eine Herausforderung für Cassandra ist die Implementierung zum Erzeugen und zur Persistenz von Nummernsequenzen. Diese benötigt man zum Beispiel, um applikationsweit eineindeutige Nummern/IDs zu generieren. Ist dies in einem RDBMS ein Standard, lässt sich diese Funktionalität mit Cassandra aufgrund der Verteilung der Daten (Partitionstoleranz) und des Konsistenzlevels (Eventual Consistency) nur sehr schwer umsetzen beziehungsweise bei hohem Konsistenzlevel gar nicht abbilden. Für diese Art von Operationen sind klassische SQL-Datenbanken klar im Vorteil.

WIE FUNKTIONIERT CASSANDRA?

Apache Cassandra legt die Daten in sogenannten Key Value Stores (Schlüssel-Wert-Speicher) ab. Der Schlüssel wird einmalig beim Erstellen einer Tabelle angelegt und kann nicht mehr ge-

ändert werden. Mit diesem Schlüssel ist definiert, wie Cassandra die Daten innerhalb des Clusters beim Schreiben verteilt (Partitionierung) und beim Lesen über den Schlüssel wieder auffinden kann. Der Primary Key besteht aus zwei Teilen:

1. Dem Partition Key, der festlegt, auf welcher Node die Zeile im Cassandra-Verbund geschrieben wird,
2. Dem Cluster Key, über dessen Attribute weitere Einschränkungen (beispielsweise Von-bis-Abfragen) durchgeführt werden können.

Der Partition Key muss beim Lesen von Daten immer komplett angegeben werden, damit die entsprechenden Datensätze innerhalb des Clusters gefunden werden kann (partitionsweise Selektion).

Beide Schlüsselteile (Partitition- und Cluster Key) können sich dabei jedoch aus mehreren Attributen (Feldern) einer Tabelle zusammensetzen (Compound Key). Ein selektierbares Attribut kann dabei entweder nur Teil des Partition Keys oder nur Teil des Cluster Keys sein. Gibt es mehrere Partition Key-Bestandteile, werden diese durch eine Klammer verbunden.

Beispiel:
PRIMARY KEY((column1, column2), column3, column4)
Beim Lesen von Datensätzen sind ausschließlich folgende Kombinationen möglich:

column1 (Partition Key)	column2 (Partition Key)	column3 (Cluster Key)	column4 (Cluster Key)
■	■		
■	■	■	
■	■	■	■

Das Weglassen aller Schlüssel kommt einer Selektion über alle Datensätze gleich. Das sorgt jedoch auf der Client-Seite für eine unter Umständen extrem hohe Speicherauslastung bei Empfang der Datensätze und auf der Server-Seite (beim Coordinator) ebenfalls für eine sehr hohe Speicherauslastung und eine hohe CPU-Last. Bei Tabellen mit vielen Einträgen wird diese Abfrage in den meisten Fällen zu einem Time-out und damit zu einem Fehler führen.

Während sich die selektierbaren Kriterien in jeweils eigenen Spalten befinden müssen, wird der abzurufende Datensatz (Value) in eine einzige Spalte geschrieben. Dadurch ist eine extrem hohe Geschwindigkeit beim Schreiben und Auffinden von Datensätzen im Cluster gewährleistet, jedoch muss der Schlüssel für das Auffinden von Datensätzen immer exakt angegeben werden.

Beim Lesen und Schreiben von Daten kann jeweils festgelegt werden, ob für den jeweiligen Vorgang eher die Konsistenz der Daten im Cluster oder die Verfügbarkeit im Vordergrund steht. Für diesen Zweck gibt es in Cassandra die Angabe des Consistency-Levels.[8]

CONSISTENCY LEVEL[9]

The Cassandra consistency level is defined as the minimum number of Cassandra nodes that must acknowledge a read or write operation before the operation can be considered successful.

Der Konsistenz-Level von Cassandra definiert, wie hoch die Mindestanzahl von Cassandra Nodes ist, die einen Lese- bzw. Schreibvorgang bestätigen müssen, damit dieser Vorgang als erfolgreich durchgeführt gilt.

Die technische Einfachheit von Cassandra schränkt die Benutzbarkeit für Entwickler mit der Erfahrung klassischer Datenbanksysteme erst einmal ein. Einerseits muss man die Verteilung der Daten innerhalb des Clusters im Auge behalten (Wahl des Partition Keys), andererseits muss das Tabellen- und Schlüsseldesign so gewählt sein, dass die fachlichen Anforderungen der Anwendung umgesetzt werden können. Bedenkt man, dass mit Cassandra exakte Abfragen ausschließlich auf dem oder den Schlüssel(n) möglich sind, ist es notwendig, hier neue Wege zu gehen.

Die Selektion von Datensätzen über mehrere Datenfelder erreicht man unter anderem mit:

1. Metatabellen
Mittels Metatabellen kann man die Selektionskriterien so gestalten, dass die fachlichen Anforderungen erreicht werden können. Metatabellen funktionieren in diesem Falle wie ein Zeiger auf den Hauptdatensatz. So kann mit verschiedenen wählbaren Schlüsseln jeweils der Schlüssel für den Hauptdatensatz selektiert werden, um letztendlich auf den Hauptdatensatz zugreifen zu können.

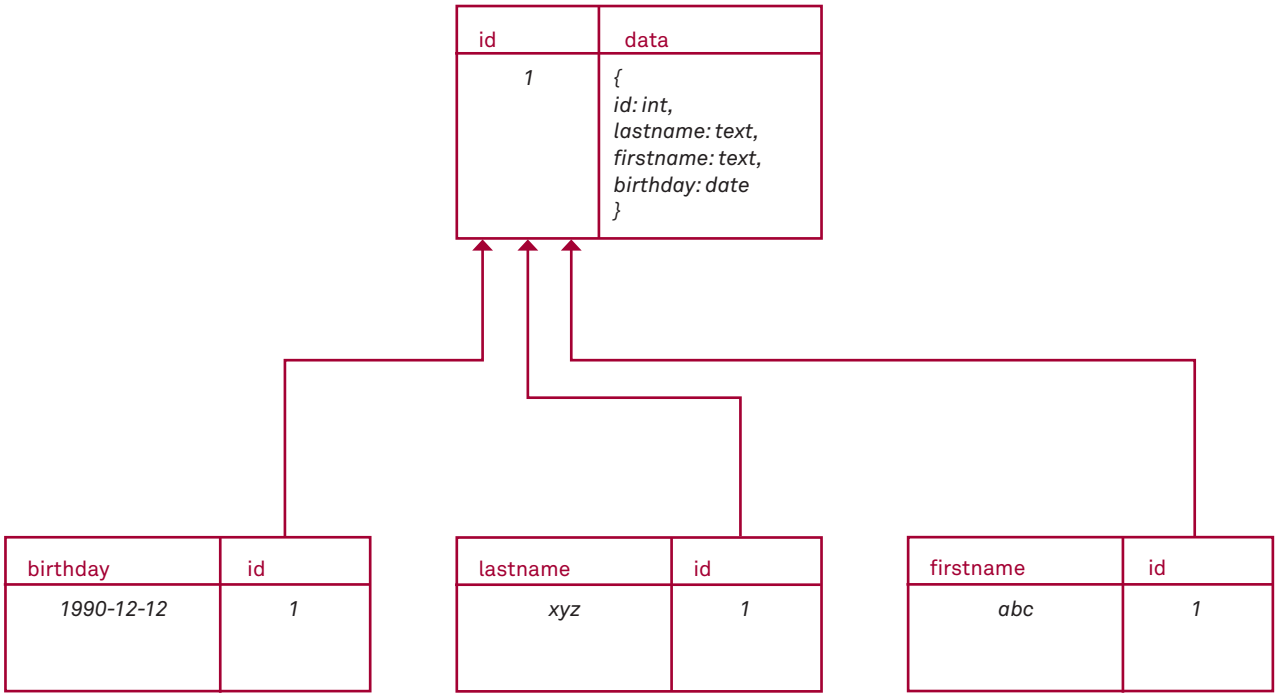


Abbildung 1: Beispieldarstellung Selektierbarkeit mittels Metatabellen

Wählt man dieses Vorgehen, sollte man immer beachten, dass a) beim nachträglichen Hinzufügen weiterer Meta-/Suchtabellen immer ein vollständiger Migrations-Job durchgeführt werden muss, um die neue Tabelle zu füllen. In Cassandra gibt es einen solchen Auto-Mechanismus nicht.
b) je nach gewählter Komplexität der Fachlichkeit immer mehrere Selektierungen notwendig sind, um die Ergebnisse anzeigen zu lassen oder verarbeiten zu können.

2. Suchindex
Ist absehbar, dass die Durchsuchbarkeit des gespeicherten Datenmodells gegeben sein muss, lässt sich das auch über Metatabellen nicht mit adäquatem Aufwand abbilden. Für diesen Anwendungsfall empfiehlt sich der Einsatz einer Suchindex-Komponente. Ein solcher Suchindex bietet von Haus aus viele Möglichkeiten der Filterung und Suche inklusive Relevanz der Ergebnisse. Als Beispiele seien hier Elasticsearch[10] oder SOLR[11] genannt. Hat man Datastax Enterprise[12] (kommerzielle Variante von Cassandra) im Einsatz, wird hier der SOLR-Suchindex mitgeliefert.

Weitere Möglichkeiten eines angepassten Zugriffs auf die Daten sind die Verwendung von Materialized Views oder der Einsatz eines sogenannten (Secondary) Index in Cassandra. Materialized Views befinden sich jedoch noch in der Betaphase und sind nicht für den produktiven Einsatz empfohlen. Gegen die Verwendung von Indizes sprechen technische, durch Cassandra bedingte, Einschränkungen.

CASSANDRA ALS VERTEILTES SYSTEM (EVENTUAL CONSISTENCY)

Ein wichtiger Grundsatz beim Einsatz von verteilten Systemen ist das sogenannte „CAP-Theorem“[13], das besagt, dass nie alle drei Eigenschaften, also **C**onsistency (Konsistenz), **A**vailability (Verfügbarkeit) und **P**artition Tolerance (Ausfallsicherheit), in einem verteilten System gleichzeitig garantiert werden können. Bei Apache Cassandra wird das A und das P garantiert, sofern die Anzahl Nodes im Cluster > 1 und der Replikationsfaktor entsprechend größer 1 gewählt ist. Cassandra verfolgt dabei den Ansatz der Eventual Consistency (keine Konsistenzgarantie im Cluster), was vereinfacht bedeutet, dass ein Datensatz irgendwann konsistent (das heißt über alle Replikas gleich) sein wird, sofern nur eine hinreichend lange Zeit ohne Schreibvorgänge und ohne Fehler vorausgesetzt werden kann.[14]

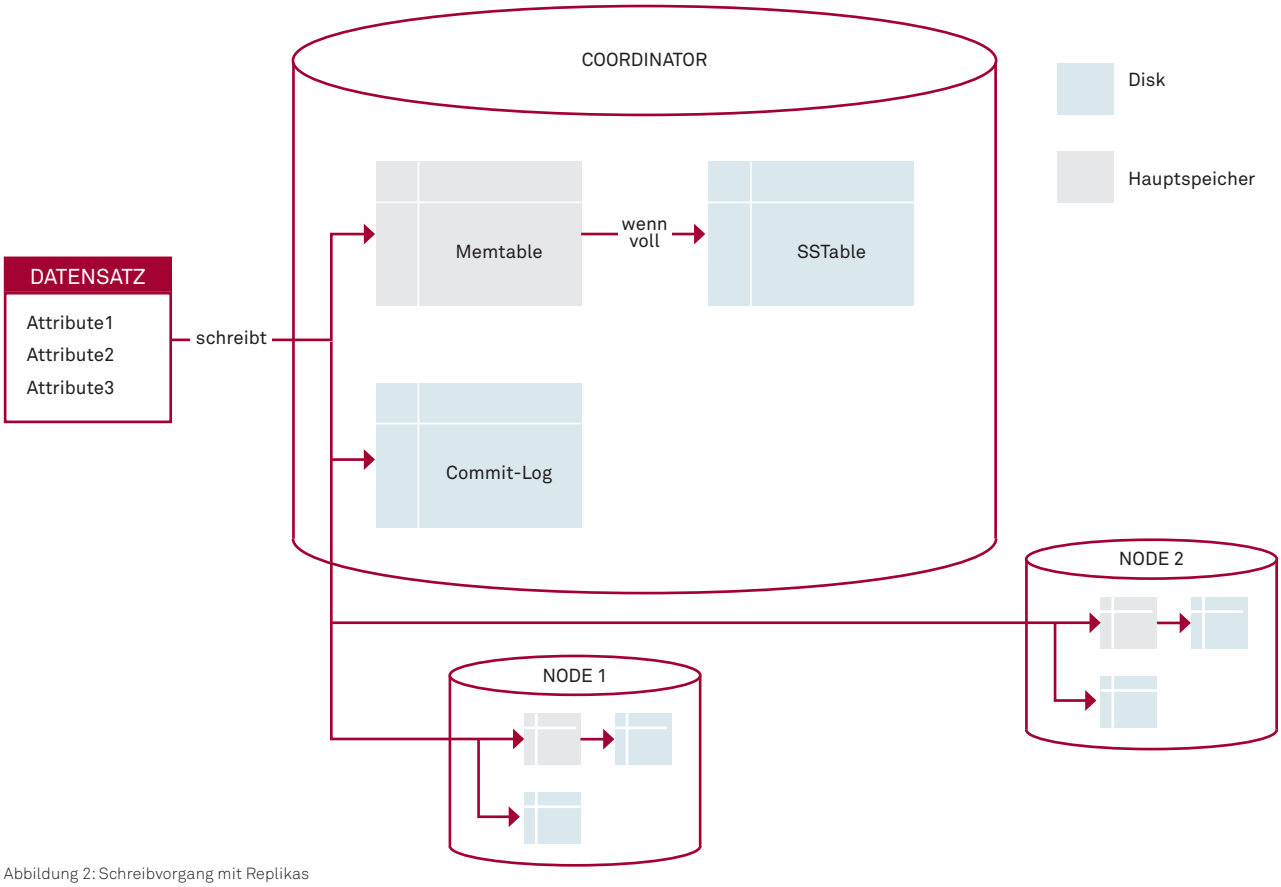


Abbildung 2: Schreibvorgang mit Replikas

EVENTUAL CONSISTENCY IN DER PRAXIS

Wird ein Datensatz geschrieben, speichert der Coordinator (siehe Glossar) den Datensatz im Commit-Log. Beim unerwarteten Ausfall einer Node können die Daten aus dem Commit-Log in die Memtable (siehe Glossar) zurückgeschrieben werden, um hier größtmögliche Konsistenz der Daten zu wahren. Bei der Memtable handelt es sich um das Teilabbild der Daten im Hauptspeicher, da der immer noch um Faktoren schneller ist als die schnellsten Solid State Disks. Gleichzeitig mit dem Schreiben in das Commit-Log verteilt der Coordinator den Datensatz auf (je nach Replikationsfaktor) den oder die Replika-Nodes. Ist die Memtable voll, werden die Daten in die SSTable (String Sorted Table) auf Disk übertragen. Während der Verteilung der Daten auf die verschiedenen Nodes ist es somit möglich, dass bei einer Abfrage und verschiedenen technischen Parametern (Konsistenzlevel beim Lesen, unterschiedliche Koordinatoren pro Verbindung, Anzahl der Replikas) für einen Zeitraum (bis alle Nodes denselben Datenstand haben) unterschiedliche Ergebnisse aus Cassandra zurückgeliefert werden. Diesen Zustand nennt man „eventual consistent“.

GLOSSAR

Cluster	Verbund von einzelnen Cassandra Nodes
Node	Eine Cassandra-Service-Instanz
Coordinator	Erster Kontaktpunkt (Verbindungsschnittstelle) einer Applikation mit Cassandra; jeder Node eines Clusters kann Coordinator sein.
Replikations-faktor	Wert, der angibt, über wie viele Nodes ein Datensatz im Cluster verteilt wird
Partition	Speicherplatz einer Tabelle auf einer Node
Keyspace	Fachliche Einordnung von Tabellen in einem Cassandra-Verbund
Replika	Gespeicherte Kopien eines Datensatzes im Cluster (für Ausfallsicherheit)
Commit-Log	Zwischenspeicher (auf Disk) einer Cassandra Node, der für Back-up-Zwecke verwendet wird
Memtable	Zwischenspeicher (im RAM) einer Cassandra Node, der auf Disk (SSTable) übertragen wird, wenn er voll ist
SSTable	String Sorted Table; Ablageort der Daten auf Disk einer Cassandra Node
Wide-Row-Datenspeicher	Cassandra zählt zu dieser Kategorie. Hier werden Daten in Spalten abgelegt (wie in klassischen SQL-Datenbanken). Das Gegenstück hierzu sind beispielsweise dokumentenbasierte Datenspeicher (Elasticsearch, MongoDB).

CASSANDRA-VERSIONEN

Zurzeit existieren zwei Lizenzmodelle für Cassandra-Datenbanken.

Apache Cassandra (Open-Source-Version im Apache-License-Modell)
Mit dieser Version ist es möglich, eine vollumfängliche, über Rechenzentrumsgrenzen hinweg verteilte Datenspeicherlösung zu implementieren. Ebenso bietet diese Version für Softwareentwickler die Möglichkeit, während der Entwicklung verschiedene Implementierungen mit Cassandra zu testen, ohne dass Lizenzkosten anfallen. Apache Cassandra steht als Docker-Container[15] zur Verfügung, wodurch es beispielsweise für Softwareentwickler oder Mitarbeiter des Betriebs sehr einfach möglich ist, einen oder mehrere Cassandra Nodes im Verbund zu betreiben, um eine Systemlandschaft zu simulieren.

DSE (Datastax Enterprise, lizenzpflichtige, nicht kostenlose Version)[16]
Die Basis-Software entspricht Apache Cassandra, jedoch erhält der Kunde erweiterten Support durch die Firma Datastax. Man erhält optimierte Treiber, erweiterte Konnektivitäten und zusätzliche Softwarepakete. Gerade beim Betrieb größerer und großer Datenbanklandschaften über Rechenzentrumsgrenzen hinweg sollte der Einsatz der lizenzpflichtigen Software erwogen werden.

FAZIT

Werden Softwaresysteme entworfen, stellt sich unweigerlich die Frage, welche Persistenz man wählt. Wenn im Vorfeld darüber Klarheit herrscht, dass große Datenmengen anfallen werden, sich der genaue Umfang jedoch nicht abschätzen lässt, sollte man den Einsatz des verteilten Datenspeichersystems Cassandra in Betracht ziehen. Durch die einfache Skalierbarkeit, hohe Ausfallsicherheit und sehr hohe Geschwindigkeit ist es bestens für den Einsatz im Big-Data-Umfeld geeignet.

Gleichzeitig verlangt Cassandra sowohl vom Betrieb als auch von der Softwareentwicklung ein hohes Maß an Lernbereitschaft. Gerade wenn bei Entwicklung und Betrieb der Fokus bislang auf klassischen RDBMS lag, müssen jetzt beide Seiten voneinander lernen, um das System so optimal wie möglich nutzen zu können und Fehler zu vermeiden.

Eine falsch genutzte Cassandra-Datenbank kann auf allen Seiten für sehr viel Frustration sorgen und das Beheben handwerklicher Fehler kann gerade am Anfang sehr zeit- und kostenintensiv beziehungsweise im späteren laufenden Betrieb nahezu unmöglich werden.

Cassandra ist auch nicht für alle Einsatzszenarien gedacht. Steht eine hohe transaktionale Sicherheit beziehungsweise Konsistenz der Daten im Vordergrund, ist man bei einem klassischen RDBMS besser aufgehoben. Dies trifft auch dann zu, wenn sich gleiche Datensätze oft ändern oder Datensätze häufig gelöscht werden.

Für den Betrieb als verteilter Datenspeicher im eigenen Rechenzentrum ist Cassandra derzeit alternativlos. Es existiert zwar mit SkyllaDB[17] eine von Cassandra abgewandelte Version, allerdings ohne professionellen Support. Grundsätzlich andere Datenspeichermethoden, wie beispielsweise MongoDb[18], die Daten als Dokumente speichert, oder Redis[19], bei der es sich um eine In-Memory-Datenbank handelt, sollten zumindest als Vertreter der NoSQL-Datenbanken auch für das Einsatzszenario wie bei Cassandra in Erwägung gezogen werden.

Wird der Einsatz in der Public Cloud erwogen, stehen hier zum Beispiel bei Amazons Cloud AWS die DynamoDB[20] oder bei Microsoft Azure die CosmosDB[21] beziehungsweise bei Google BigTable[22] als Vertreter der NoSQL-Wide-Row-Datenspeicher zur Verfügung. ●

1 Süddeutsche Zeitung, 23.09.1995.
2 http://cassandra.apache.org/ (abgerufen am 28.02.2020).
3 https://www.facebook.com/note.php?note_id=24413138919 (abgerufen am 28.02.2020).
4 https://www.infoq.com/news/2014/10/netflix-cassandra/ (abgerufen am 28.02.2020).
5 https://academy.datastax.com/planet-cassandra/nosql-performance-benchmarks (abgerufen am 28.02.2020).
6 https://de.wikipedia.org/wiki/DevOps (abgerufen am 28.02.2020).
7 https://de.wikipedia.org/wiki/Domain-driven_Design (abgerufen am 28.02.2020).
8 https://docs.datastax.com/en/ddac/doc/datastax_enterprise/dbInternals/dbIntConfigConsistency.html (abgerufen am 28.02.2020).
9 https://docs.apigee.com/private-cloud/v4.17.09/about-cassandra-replication-factor-and-consistency-level#aboutthecassandraconsistencylevel (abgerufen am 28.02.2020).
10 https://www.elastic.co/de/ (abgerufen am 28.02.2020).
11 https://lucene.apache.org/solr/ (abgerufen am 28.02.2020).
12 https://www.datastax.com/products/datastax-enterprise (abgerufen am 28.02.2020).
13 https://de.wikipedia.org/wiki/CAP-Theorem (abgerufen am 28.02.2020).
14 https://de.wikipedia.org/wiki/Konsistenz_(Datenspeicherung)#Verteilte_Systeme (abgerufen am 28.02.2020).
15 https://hub.docker.com/_/cassandra (abgerufen am 28.02.2020).
16 https://db-engines.com/de/system/Cassandra%3BDatastax+Enterprise (abgerufen am 28.02.2020).
17 https://www.scylladb.com/ (abgerufen am 28.02.2020).
18 https://www.mongodb.com/de (abgerufen am 28.02.2020).
19 https://redis.io/ (abgerufen am 28.02.2020).
20 https://aws.amazon.com/de/dynamodb/ (abgerufen am 28.02.2020).
21 https://azure.microsoft.com/de-de/services/cosmos-db/ (abgerufen am 28.02.2020).
22 https://cloud.google.com/bigtable/ (abgerufen am 28.02.2020).

DATEN FÜR DIE ZUKUNFT DES GEMEINWESENS

Warum wir eine Datendemokratie etablieren müssen

| von JÜRGEN FRITSCHE

Daten können einen in höchstem Maße zielgerichteten und auch effizienteren Einsatz von Ressourcen, Maßnahmen, Produktionsmitteln und Personal ermöglichen. Datendemokratie soll – aufbauend auf europäischen Werten und einem europäischen Demokratieverständnis – die Potenziale vorhandener Daten für die wirtschaftliche, soziale und ökologische Entwicklung heben. Eine Datendemokratie zu schaffen und zu fördern, ist daher eine bisher vernachlässigte wesentliche und wichtige Aufgabe für Politik und Zivilgesellschaft.

Daten sind heute von essenzieller Bedeutung für die Wirtschaft und in der Gesellschaft insgesamt – und ihre Bedeutung wächst: Mit der Entwicklung künstlicher Intelligenz steigt der Bedarf an Daten, und mit der Durchsetzung des Internet of Things nimmt die Fülle vorhandener Daten weiter stark zu. Die EU geht von einem Wachstum weltweit gespeicherter Daten um den Faktor fünf auf rund 175 Zettabyte bis zum Jahr 2025 aus.[1]

Schon lange werden Daten erhoben und Handlungen daraus abgeleitet. Neu sind Menge und Präzision der Daten – in Verbindung mit massiven Ungleichheiten hinsichtlich Datenbesitz und -zugriff sowie der Möglichkeiten ihrer automatisierten Auswertung. Und diese Ungleichheit bestimmt heute auch, wer die Regeln vorgibt und wo die Wertschöpfung erfolgt.

DAS GESICHT ALS PASS

Die Gesichtserkennung, auch beim Smartphone inzwischen Standard, ist vielleicht das beste Beispiel für ein asymmetrisches Datensammeln, um den Handlungsbedarf einer demokratischen Gesellschaft deutlich zu machen. Apples „Face ID" erfasst 30.000 Punkte und erstellt eine detaillierte 3-D-Tiefenkarte des Gesichts. Face ID, so die werbliche Aussage des Unternehmens, würde den Nutzer immer und zweifelsfrei erkennen, selbst dann, wenn Freunde ihn nicht mehr wiedererkennen. Natürlich verwendet nicht nur Apple solche Technologien: „Rekognition" von Amazon erkennt seit 2016 Inhalte in Videos, Facebook identifiziert seit 2018 Gesichter in Fotos. Und in China werden im Abstand von 30 Sekunden die Gesichter von Schülern gescannt, um zu überprüfen, ob sie den Unterricht aufmerksam verfolgen.[2]

Nicht nur in China, auch in Amerika, Großbritannien und Deutschland, ja überall auf der Welt ist der öffentliche Raum voller Kameras. Und das Internet enthält Milliarden von Fotos von Menschen, die beispielsweise in sozialen Netzwerken hochgeladen wurden. Das Unternehmen Clearview AI hat eine biometrische Datenbank mit drei Milliarden Bildern erstellt, die im Internet verfügbar waren. Es ist naheliegend, aus diesen Daten ein Businessmodell zu machen. Kunden hat Clearview AI etwa in amerikanischen Ermittlungsbehörden, die Software wurde mehr als 600 Behörden angeboten.[3] Es ist davon auszugehen, dass die Bilder mit weiteren frei verfügbaren Daten zur Identifikation von Personen angereichert wurden.

Australien hat ein System mit dem Namen „SmartGate" eingeführt, das die Einreise auf Basis von Gesichtserkennung ohne die Vorlage von Papieren ermöglicht.[4] Das Erkennen kann jedoch fehlschlagen, zum Beispiel bei Verletzungen im Gesicht. Dasselbe gilt für Fingerabdrücke bei verletzten Fingern. Der Mensch wird biometrisch unleserlich – aber ist er dann auch ohne Staatsbürgerschaft? Das australische Innenministerium sagt, wenn Finger fehlen, müssen die verbleibenden Finger gescannt werden, bei Verletzungen ist zu warten, bis die Fingerspitzen verheilt sind. Wäre die biometrische Erkennung die einzige Möglichkeit, sich auszuweisen, stünde die verletzte Bürgerin, der verletzte Bürger außerhalb des Systems, außerhalb des Gesetzes.

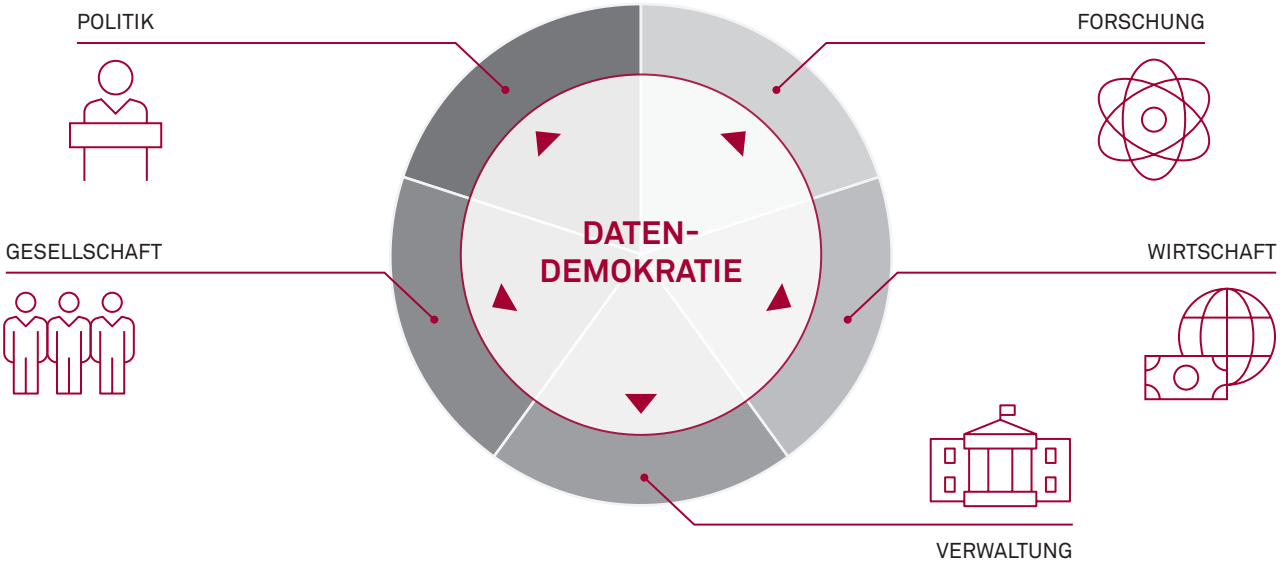


Abbildung 1: Datendemokratie und Gemeinwesen

CODE IS LAW

Das Gesetz ermöglicht dem Individuum zu entscheiden, ob es dem Gesetz folgt. Dies beinhaltet immer auch die Möglichkeit der Zuwiderhandlung. Gesetze schützen das Individuum vor anderen, vor allem aber auch vor Machtmissbrauch. Und das Recht ist auslegbar. Wenn der Staat Regelungen auf Basis von Daten und automatisierter Auswertung trifft, gibt er das Prinzip der Rechtsstaatlichkeit auf, das für eine Demokratie in unserem Verständnis konstitutiv ist. Denn Software-Architektur ist starr, sie lässt keinen Spielraum zu, minimiert Freiheiten. Somit entspricht sie eher struktureller Gewalt. Der Einsatz von weiteren Machtmitteln ist überflüssig.

Wer in der US-Flugverbotsliste geführt ist, wird nicht mehr über amerikanisches Hoheitsgebiet fliegen können. Das passiert nicht nur Terrorverdächtigen. Als verdächtig klassifizierte Wörter in Social-Media-Posts oder bestimmte Bewegungen beim Betreten des Flughafens können auch unbescholtenen Bürgerinnen oder Bürgern einen solchen Eintrag bringen. Die Kriterien sind nicht transparent. Die Software, die die Daten dort ablegt und eine Löschung so schnell nicht vorsieht, ist das Gesetz.

Das Problem ist nicht neu – und auch nicht die Einsicht dessen. Das Sachbuch „Code And Other Laws of Cyberspace" des US-Verfassungsrechtlers Lawrence Lessig ist bereits 1999 erschienen. Flugverbotslisten und Gesichtserkennung sind heutige Beispiele für eine technokratische Verwendung von Daten, die Rechtsstaatlichkeit und bürgerliche Freiheiten aussetzt. Sie mahnen zu Zurückhaltung und Umsicht bei der Erfassung und Nutzung der Daten von Bürgern.

FREIHEIT STATT ÜBERWACHUNG

Politik und Verwaltung, aber auch Wirtschaft und Gesellschaft müssen einen Weg im Umgang mit Daten finden, der das Gemeinwesen in eine lebenswerte Zukunft führt. Daten eröffnen viele Chancen in allen gesellschaftlichen Bereichen. Aber nur auf Basis einer Datendemokratie lassen sie sich im Einklang mit unserer Rechtsordnung und einem europäischen Werteverständnis nutzen. Es geht darum, Regeln zu definieren und mithilfe dieser Regeln die Potenziale zu heben – zum Wohle aller.

AUS DATEN WISSEN SCHAFFEN

Forschung ist die Basis für die Entwicklung neuer Lösungen in allen Bereichen, sie ist damit auch Basis für die Entwicklung von Wohlstand und Gemeinwesen. Insbesondere die Forschung zu künstlicher Intelligenz ist auf Daten angewiesen. Aber ihre Ergebnisse weisen auch einen Weg für die Nutzung von Daten insgesamt.

Die deutsche Strategie zur Förderung von KI wurde im Dezember 2018 auf dem Digitalgipfel der Bundesregierung offiziell vorgestellt.[5] Die Daten der Verwaltung wären eine gute Quelle für KI-Forschung, natürlich auch für Start-ups und die Wirtschaft insgesamt, wenn sie maschinenlesbar verfügbar gemacht würden. Um dies zu gewährleisten, ist noch einiges zu tun. Die Weiterentwicklung des Open-Data-Umfeldes hat die Bundesregierung in ihrem Zweiten Aktionsplan Open Government im Herbst 2019 als wichtigen Baustein benannt.[6] Eine dedizierte Open-Data-Strategie folgt im Zusammenhang mit der Datenstrategie der Bundesregierung.

Tatsächlich sind neben der KI-Forschung auch die allermeisten anderen Forschungsfelder auf Daten angewiesen. Weitreichende Erkenntnisse nicht nur zur Verbreitung, sondern auch etwa zu Krankheitsverläufen und relevanten gesundheitlichen Faktoren verspricht sich das Robert-Koch-Institut – und alle, die an Impfstoffen oder Medikamenten arbeiten – von den freiwilligen Datenspenden der Bürger, die im Zusammenhang mit der sogenannten Corona-App abgegeben werden können.

Datenspenden sind auch Grundlage für die Arbeit der HippoAI Foundation, ebenfalls tätig im Gesundheitsbereich, die die Qualität der gesammelten Daten sichert und sie als offene Daten forschenden Institutionen oder Unternehmen zur Verfügung stellt. Die Datensätze können unentgeltlich genutzt werden – unter der Voraussetzung, dass das daraus gewonnene Wissen „demokratisiert" wird, der Allgemeinheit also zur Verfügung steht.[7]

Was geschieht, wenn Daten nicht mehr automatisch demjenigen gehören, der sie sammelt, sondern wenn sie – anonymisiert und gemäß DSGVO – allen zur Verfügung stehen? Das eigentliche Geschäftsmodell liegt dann nicht mehr in der Datensammlung und Vermarktung, sondern in dem Wissen, das daraus gewonnen wird. Das ist ein Aspekt von Datendemokratie.

WISSEN UM ZU HANDELN

Die Stadt Boston hat einen Index entwickelt, der die Gesamtleistung der Stadt anzeigt. Der „Boston City Score"[8] setzt sich aus Einzelindizes wie Anzahl der Schlaglöcher, Verkehrsstaus, Straftaten oder Reaktionszeit der städtischen Services zusammen. Hinzu kommen Daten zu öffentlicher Sicherheit, Bildung, Leistungen von Gesundheitsdiensten und zur Wählerzufriedenheit.

Ein Mittelwert aller Einzelindizes bildet den Gesamtindex. Ein Wert von 1,0 bedeutet, dass alles normal funktioniert. Ein Wert niedriger als 1 signalisiert Handlungsbedarf, ein Wert höher als 1 ist sehr gut. All dies ist nahezu in Echtzeit im Internet öffentlich. So kann sich jeder darüber informieren, was in der Stadt los ist. Und die Administration weiß, was zu tun ist.

ERKENNEN UM ZU ENTSCHEIDEN

In Hamburg gibt es ein integriertes, medienbruchfreies System zur Bürgerbeteiligung, das sowohl online als auch mit digitalen Planungstischen bei realen Zusammenkünften zum Einsatz kommt. Bürgerinnen und Bürger können von zu Hause aus, mobil oder in Veranstaltungen über das digitale Partizipationssystem DIPAS Karten, Luftbilder, Pläne, 3-D-Modelle und Geodaten abrufen und auf Grundlage dieser Verwaltungsdaten ein präzises Feedback zu Planungsvorhaben geben. Daten werden damit ein Mittel zur Teilhabe an politischen Entscheidungen, zur Wahrnehmung demokratischer Rechte also.

DATEN UND POLITIK

Die Politik hat die Bedeutung von Daten für uns alle erkannt und den Handlungsbedarf adressiert. Die EU-Kommission hat ihre Datenstrategie vorgestellt, die Datenstrategie der Bundesregierung soll nach einer Online-Konsultation zu den Eckpunkten in diesem Herbst veröffentlicht werden. Beide politischen Willensbekundungen enthalten einige Elemente von Datendemokratie. EU-Binnenmarktkommissar Thierry Breton kommentiert die Datenstrategie der EU: „Der Daten-‚Schatz' darf nicht nur der Industrie nützen. Die Gesellschaft insgesamt muss von der Datenrevolution profitieren: Das Gesundheitssystem, öffentliche Daseinsvorsorge und Maßnahmen zum Umwelt- und zum Klimaschutz sind dringend auf eine bessere Datenbasis für Entscheidungen angewiesen. Wir Menschen sollen durch mehr und bessere Daten in die Lage versetzt werden, bessere Entscheidungen zu treffen. Wir steuern die Verwendung der Daten, nicht die Daten uns. Dann liegt das Beste der Datenrevolution noch vor uns."[9]

In guten beziehungsweise besseren Entscheidungen durch Daten, in sogenannten evidenzbasierten Entscheidungen, liegt die große Chance für die Politik: Wenn die Entscheider in der Politik wissen, wo beispielsweise Breitbandinternet vorhanden ist und wo gleichzeitig die medizinische Versorgung dünn ist, dann ist auch klar, wo sinnvollerweise Modellregionen für Telemedizin gefördert werden sollten. Auch für politische Herausforderungen wie den Klimawandel liegen Chancen in der Datenanalyse. Mit Ökosystemmodellen und anderen Simulationen lassen sich die Auswirkungen politischer Handlungsalternativen durchspielen.

Die Beispiele Boston und Hamburg zeigen noch einen weiteren Pfad: Transparenz und Beteiligung schaffen Vertrauen, gute Entscheidungen schaffen Akzeptanz, mit dem öffentlichen Zugang zu Informationen lassen sich Bürgerbeteiligungen sinnvoll umsetzen. Kurz: Daten können das Vertrauen in die Demokratie stärken.

DATEN FÜR EINE EFFEKTIVERE VERWALTUNG

Immer wieder ist von einem Digital-Check für Gesetze die Rede. Denn eine gute politische Entscheidung muss, um Akzeptanz und Zustimmung zu finden, auch umsetzbar sein. Die Einführung der Grundrente werde voraussichtlich 8,5 Millionen Euro kosten, stellte der Normenkontrollrat fest.[10] Denn die IT-Verfahren zum notwendigen Datenaustausch zwischen Finanzverwaltung und Rentenversicherung gibt es noch nicht. Die Prüfung müsste aktuell in vielen Fällen manuell vorgenommen werden, weil erforderliche Daten nicht vorliegen oder auf diese nicht zugegriffen

werden kann. Würden entsprechende Verfahren nicht spätestens bis zum Sommer entwickelt oder tausendfach neues Personal angestellt, wackelt der Start der Grundrente Anfang des nächsten Jahres.

Auch das EU-weit vorgesehene Once-Only-Prinzip fordert, dass unterschiedliche Behörden auf einmal erhobene Daten zugreifen können. Der Zugriff auf die im engsten Sinne verwaltungseigenen Daten ist aber nur ein Aspekt davon, wie die Verwaltung durch Daten zu einem effektiveren und effizienteren Handeln kommen kann. Offensichtliche Potenziale liegen darüber hinaus vor allem im kommunalen Bereich.

DATENSCHATZ KOMMUNE

Schon heute werden im städtischen Raum reichlich Daten erzeugt. Und es kommen immer neue Datenquellen hinzu, im vergangenen Jahr etwa mit der Einführung von E-Rollern. Bei denen geht nichts ohne die App, in der man sich registriert und Zahlungsdaten hinterlegt. Der Verleiher speichert jeden Vorgang: Wann, wo und von wem wurde geliehen, wohin wurde gefahren und wie schnell? Jeder Roller ist mit GPS ausgestattet. Wer einen solchen E-Scooter mietet, akzeptiert mit den Geschäftsbedingungen die Verwertung dieser Daten durch den Anbieter. Es bleibt unklar, ob auf dieser Basis tatsächlich nur der jeweilige Dienst optimiert wird. Für Belange der Gesellschaft stehen die Daten heute nicht zur Verfügung, sie gehören Privatunternehmen. Kommunen, die Genehmigungen erteilen, sichern sich in der Regel keine Rechte an Daten von Dienstanbietern. Gleiches gilt für GPS-Daten aus Navigationsgeräten oder Bewegungsdaten von Smartphones. Um an dieser Situation etwas zu ändern, müsste der Automatismus, mit dem die Daten den Unternehmen zufallen, die sie erheben, aufgebrochen werden. Dafür können im Einzelfall bereits Verhandlungen mit Anbietern ausreichen. Darüber hinaus werden jedoch auch gesetzliche Regelungen erforderlich sein, um dem Staat beziehungsweise seinen Bürgern Nutzungsrechte für im öffentlichen Raum erhobene Daten zu sichern – und zwar von Beginn an und am besten in Echtzeit. Nur per Gesetz wird sich die Datenmacht etablierter Anbieter, die den Markt dominieren, aufheben lassen. Auch deren nie gelöschte, historische Daten sind ein riesiger Datenschatz.

Der Staat verfügt also über reichlich Daten, wenn er die im öffentlichen Raum erhobenen Daten als hoheitlich betrachtet und sich die Nutzungsrechte sichert. Das gilt insbesondere für Daten, die im Betrieb einer sogenannten Smart City entstehen. Die Integration intelligenter Sensoren in Aspekte kommunalen Handelns, von der Parkplatzbewirtschaftung und dem Verkehrsmanagement über die Müllabfuhr bis hin zur Sicherung der Luftqualität und Bewässerung von Grünanlagen, kann viele Leistungen verbessern. Barcelona hat die Routen der Müllabfuhr am Bedarf, also den vollen Tonnen, ausgerichtet und optimiert. Das spart Ressourcen und verringert den Schadstoffausstoß. Die dazu notwendige Infrastruktur inklusive der Daten gehört dabei der Stadt Barcelona. Bürger, Unternehmen und andere Interessenten können sie nutzen, Stadt und Einwohner bleiben jedoch die wahren Eigentümer und entscheiden über Zugriff, Datenschutz usw.[11] Das ist Datendemokratie.

MIT DATENDEMOKRATIE DIE ZUKUNFT SICHERN

Das müssen Deutschland und die EU schaffen: auf Basis demokratischer Werte Daten nutzen und auch KI entwickeln – um damit ein Alleinstellungsmerkmal und einen Wettbewerbsvorteil zu erlangen und damit Wohlstand zu sichern und zugleich die Gesellschaft insgesamt nachhaltig weiterzuentwickeln. ●

1 https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_de.pdf (abgerufen am 19.07.2020).
2 https://de.wikipedia.org/wiki/Face_ID; https://en.wikipedia.org/wiki/Amazon_Rekognition; https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/gesichtserkennung-bei-facebook-das-sollten-nutzer-wissen-23818; https://www.deutschlandfunk.de/alles-unter-kontrolle-chinas-intelligenter-schule-entgeht.680.de.html?dram:article_id=438868 (abgerufen am 19.07.2020).
3 https://www.zeit.de/digital/2020-01/clearview-gesichtserkennung-app-start-up-hoan-ton-that (abgerufen am 19.07.2020).
4 lhttps://en.wikipedia.org/wiki/SmartGate (abgerufen am 19.07.2020).
5 https://www.bmbf.de/files/Nationale_KI-Strategie.pdf (abgerufen am 19.07.2020).
6 https://www.open-government-deutschland.de/resource/blob/1591050/1667952/76e3507032b45db327d7427d67e70f66/zweiter-nap-data.pdf?download=1 (abgerufen am 19.07.2020).
7 https://www.gruenderszene.de/health/hippoai-ki-g4a-witte (abgerufen am 19.07.2020).
8 https://www.boston.gov/innovation-and-technology/cityscore (abgerufen am 19.07.2020).
9 https://background.tagesspiegel.de/digitalisierung/datenrevolution-warum-das-beste-erst-noch-vor-uns-liegt (abgerufen am 19.07.2020).
10 Matthias Punz, NKR: IT-Umstellung bei der Grundrente kostet Millionen, in: Tagesspiegel Background Digitalisierung (Newsletter).
11 https://hub.beesmart.city/city-portraits/smart-city-portrait-barcelona (abgerufen am 19.07.2020).


40 JAHRE
.msg
WE MAKE IT HAPPEN

Adrian Lobe: „Speichern und Strafen. Die Gesellschaft im Datengefängnis“. EINE REZENSION

| von DR. KATRIN EHLERS

ALLES UNTER KONTROLLE

Digitales Leben – Bücher zu diesem Thema füllen einige Regalmeter im gut sortierten, analogen Buchhandel. Ein Zeichen dafür, dass viele Menschen besser verstehen wollen oder Orientierung suchen: Die Explosion des Digitalen bestimmt zunehmend unseren Alltag und unser Zusammenleben. Ja, es definiert die soziale Interaktion insgesamt – und zwar in globalem Maßstab. Daten, das sogenannte Öl des 21. Jahrhunderts, sind der Treib- oder Sprengstoff, der die Entwicklung so schwindelerregend beschleunigt, nicht nur in ökonomischer Hinsicht. Europa ist sich sicher, weder den chinesischen Überwachungsstaat noch die totale Herrschaft amerikanischer Konzerne zu wollen. Diese zwei Pole allein sind Gründe genug, um kurz stopp zu sagen und sich Zeit zu nehmen – beispielsweise für ein gutes Buch. Um mehr darüber zu erfahren, was da vor sich geht und wie das funktioniert – und wie sich womöglich der scheinbare Automatismus unterbrechen und Gestaltungshoheit wiedergewinnen lässt.

Zwar liefert Adrian Lobes im Herbst 2019 erschienenes Buch „Speichern und Strafen. Die Gesellschaft im Datengefängnis“ zu dem „Was tun“ keine Antworten. Umso unnachgiebiger ist es jedoch in der Zustandsbeschreibung und -analyse. Adrian Lobe gehört zu den Mahnern. Er beschreibt in unzähligen Beispielen den Normalfall Überwachung, die alle trifft und alle einschränkt, schuldig oder unschuldig. Schon die zahlreichen Fälle fehlgeleiteter Berechnungen machen das Buch lesenswert. Doch weitergehend wird auf anschauliche Weise deutlich, dass nicht die Fehleranfälligkeit der Datenauswertung und auch nicht der gezielte Machtmissbrauch Kerne des Problems sind, sondern dass bereits die Berechnung als solche Objektivität und Alternativlosigkeit suggeriert. Technokratie als Herrschaftsform bedeutet das Ende von Politik: „Wenn aber das Verhalten von Individuen, Gruppen und der Gesellschaft als ganzer berechenbar wird, wird politische Willensbildung Makulatur. Wo alles determiniert ist, ist nichts veränderbar.“ (S. 212)

„Speichern und Strafen“ ist eine Fortschreibung von „Überwachen und Strafen“, ein erstmalig 1975 erschienenes Buch des französischen Philosophen Michel Foucault, das sich mit der Entwicklung von Strafsystemen in Europa im frühen 18. Jahrhundert beschäftigt und damit einen wesentlichen Baustein in der Entwicklung von Foucaults Herrschaftstheorie darstellt. Von zentraler Bedeu-

Adrian Lobe, Speichern und Strafen. Die Gesellschaft im Datengefängnis, Verlag C.H. Beck, München 2019

„Das Smartphone zählt unsere Schritte, die Smartwatch misst unsere Herzfrequenz, und das Smart Home detektiert Zigarettenrauch und Schimpfwörter. Endlich gibt es all diese klugen kleinen Helfer, die uns liebevoll behüten und umsorgen, unser Leben erleichtern. Falsch! Adrian Lobe zeigt, wie uns die Digitaltechnik geradewegs in ein Datengefängnis führt, das wir selbst gebaut haben und so bald nicht wieder verlassen werden."

tung ist dabei die Idee des Gefängnisses als Panoptikum, in dem der Wächter von der Mitte aus Einblick in sämtliche geöffneten Zellen hat: In jedem Moment möglicherweise Objekt der Beobachtung zu sein, reicht aus, um die Gefangenen zu disziplinieren. Vom Internet oder gar vom Internet der Dinge, von der ganzen Datensammelwut der Konzerne wusste Foucault natürlich noch nichts. Dennoch ist Foucaults Werk hochaktuell, so Lobe, „weil er darin Machttechniken beschreibt, die sich als Erklärungsfilter auch für die Analyse programmierter Gesellschaften dienstbar machen lassen." (S. 17) Das Speichern von Daten ist, wenn man dem Ansatz folgt, an sich eine nicht mehr spürbare Überwachung und somit die Vollendung der von Foucault kritisch beschriebenen Macht. Das ist der theoretische Ausgangspunkt und der Anspruch von Adrian Lobes Buch. Entsprechend beschreibt er die Datenherrschaft mit dem Vokabular aus Strafverfolgung und -vollzug: „Jedes Speichern ist Arrest […], bei [dem] Individuen für eine juristische Sekunde festgehalten werden und ihre Daten in Untersuchungshaft landen. Die Daten werden abgegriffen, untersucht und eingehend befragt. Diese permanenten Festnahmen werden nur deshalb nicht als übergriffig empfunden, weil hier nicht der physische Körper abgetastet, sondern allein der Datenkörper untersucht wird. Diese Mikro-Festnahmen, wie ich sie nennen möchte, werden sich […] zu einer panoptischen Haft verdichten." (S. 27)

Der theoretische Hintergrund gibt Lobes Ausführungen eine gewisse Eindringlichkeit und Schärfe. Die Verflechtung realer Geschehnisse und gelebter Praktiken aus einer „Gesellschaft im Datengefängnis" mit der Reflexion von soziologischen und philosophischen Befunden und Texten (nicht nur Foucaults) ist keine leichte Kost und schlägt die Leser dennoch in den Bann. In „1984", dem berühmten dystopischen Roman (und dem Todesjahr Foucaults), der auf den Erfahrungen mit Faschismus und Stalinismus beruht, spielt die Gedankenpolizei eine zentrale Rolle. In den 10er-Jahren dieses Jahrtausends ist die Gedankenpolizei Realität: Ein Facebook-Profil hat den Charakter einer Stasi-Akte (S. 144), Suchmaschinenprotokolle werden von der Polizei als Beweismaterial herangezogen. Letzteres führte 2012 zur Verhaftung und Verurteilung des „Canibal Cop" in New York. Der Polizist hatte sich mithilfe von Google über Tötungspraktiken informiert und sich in Chats über seine vermeintlichen Vorhaben ausgetauscht. Umgesetzt hat er seine Pläne nicht. 2014 wurde der Schuldspruch aus Mangel an Beweisen aufgehoben, da hatte der Mann 21 Monate in Haft gesessen. 2015 schließlich gab es einen weiteren Erfolg vor einem Berufungsgericht: Es sei nicht rechtens, jemanden wegen seiner Gedanken zu bestrafen, Fantasien, auch perverse, zu kriminalisieren, so die Urteilsbegründung. „Das Urteil atmete einen aufklärerischen Geist", kommentiert Lobe (S. 66). Der Beschuldigte war rehabilitiert, Job, Frau und Kind hatte er allerdings auf Dauer verloren. Im Buch folgt die Beschreibung eines weiteren ähnlichen, wenn auch weniger spektakulären Falles aus Deutschland.

Nach der Lektüre von „Speichern und Strafen" wird kaum jemand noch beschwichtigen, dass, wer nichts Böses getan hat, seine Daten bedenkenlos abgeben könne.

Abschließend noch ein Hinweis an alle Leserinnen und Leser, entnommen Edward Snowdens „Permanent Record": Wenn Sie das Buch online kaufen oder mit Karte bezahlen, wird die NSA das wissen. Wenn Sie es auf einem elektronischen Gerät lesen, werden die NSA-Server verzeichnen, an welchen Stellen Sie vor- oder zurückblättern oder was sie während der Lektüre im Netz nachgesehen haben.[1] ●

1 Vgl. Edward Snowden, Permanent Record, Macmillan London 2019, S. 325.

WARUM DIE DATENWISSENSCHAFTEN DIE SOZIALWISSENSCHAFTEN BRAUCHEN

| VON JOHANNES MÜLLER (CAUSE&EFFECT UG)

Es ist das Kernversprechen der künstlichen Intelligenz: Wenn wir nur genug Daten haben, können mathematische Modelle – viel besser als der Mensch – Muster erkennen, Resultate vorhersagen und Entscheidungen treffen. Doch war dieses Kernversprechen nicht eigentlich der Markenkern der Sozialwissenschaften? Komplexe Sachverhalte verstehen, Muster abstrahieren, Folgen abschätzen, um anschließend bessere Entscheidungen treffen zu können? Stellt sich die Frage, ob die Sozialwissenschaften im Kontext von KI einzig deren Auswirkungen auf Gesellschaft und Politik untersuchen und begleiten werden.

Ganz im Gegenteil: sozialwissenschaftliche Methoden werden nicht nur eine wichtige Rolle in den Datenwissenschaften spielen, vielmehr sind sie elementar für den Erfolg von Datenanwendungen im öffentlichen und dritten Sektor.

VON DER KORRELATION ZUM VERSTÄNDNIS

Bei all den großen Versprechen von maschinellem Lernen und künstlicher Intelligenz basieren deren Methoden am Ende des Tages auf linearer Algebra und Statistik. Ein Beispiel sind die viel besprochenen künstlichen neuronalen Netze: Sie erkennen Muster in großen Mengen von Daten und bieten so die Möglichkeit, neue Datenpunkte einzuordnen. Diese Muster basieren aber fast ausschließlich auf Korrelationen. Bei einigen Anwendungsfällen ist das vollkommen ausreichend – bei der Bilderkennung zum Beispiel. An anderer Stelle sind sie unterkomplex, denn sie helfen uns nicht, die Daten zu verstehen und die Ergebnisse zu interpretieren. Ein Beispiel: Ein neues Regelwerk soll helfen, Langzeitarbeitslose in den Arbeitsmarkt zu reintegrieren. Dazu werden mithilfe eines neuronalen Netzwerks und historischer Daten speziell Menschen identifiziert, bei denen eine erfolgreiche Reintegration wahrscheinlich ist.

Gemessen an der Modellgüte scheint das neuronale Netz hervorragend zu funktionieren, allerdings bleiben entscheidende Fragen unbeantwortet: Funktioniert das Regelwerk? Wie funktioniert es? Warum funktioniert es und unter welchen Umständen (nicht)? Funktioniert die Software? Wie funktioniert die Software? Warum funktioniert sie beziehungsweise wann und warum funktioniert sie nicht?

Antworten auf diese Fragen liefert das Modell – da es auf Korrelationen basiert und die Kausalität ausblendet – nicht. An dieser Stelle bieten die Sozialwissenschaften das passende Instrumentarium, nämlich kausale Wirkungsmodelle, experimentelle und quasi-experimentelle Methoden und insbesondere eine theoretische Fundierung.

KOMPLEXITÄT

Eine Grundannahme von Statistik und maschinellem Lernen ist die sogenannte „Independent and identically distributed"-Annahme: Man geht davon aus, dass sich das System, in dem die

Daten generiert werden, selbst nicht ändert. Nur so lässt sich ein gelerntes Muster auf neue Daten anwenden. Dynamische Komplexität ist damit der wahrscheinlich größte limitierende Faktor von künstlicher Intelligenz. Bei manchen Anwendungsfällen ist sie praktisch vernachlässigbar (zum Beispiel bei Anwendungen im Internet-of-Things-Bereich), in anderen ist sie elementar.

Genau das ist die Stärke von sozialwissenschaftlicher Betrachtung. Sozialwissenschaften analysieren Daten fast ausschließlich im Kontext. Sie untersuchen Veränderungen dieses Kontexts und deren Auswirkungen. Denn Daten entstehen nicht in einem Vakuum – sie werden mal mehr, mal weniger bewusst generiert. Um auf dieser Basis Einblicke zu generieren und Entscheidungen zu treffen, ist ein qualitatives Verständnis dieses Datengenerierungsprozesses, des Kontexts, unbedingt geboten.

DER MENSCH IM MITTELPUNKT

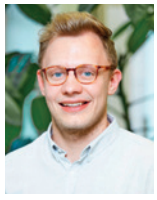
Nun zur zentralen Frage: Sollen algorithmische Systeme Entscheidungen für uns treffen? Auch hier kommt es sehr stark auf den Kontext an. In manchen Situationen sind die Risiken begrenzt. Wenn zum Beispiel ein Unternehmen mithilfe eines Algorithmus Windelwerbung gezielt an Nutzer ausspielen möchte, ist die Fehlerwahrscheinlichkeit nicht wirklich entscheidend. Finanziell ja, aber eben nur das. Wenn ein mathematisches Modell aber darüber entscheiden soll, ob ein Antrag bei einer Behörde angenommen wird oder nicht, steht viel mehr auf dem Spiel.

Das Ziel sollte daher eine datenbasierte Entscheidungsfindung sein – und nicht die Entscheidung durch Daten. Dafür müssen Daten kritisch eingeordnet und Handlungsempfehlungen zielgerichtet abgeleitet werden.

FAZIT

Der öffentliche Sektor kennt viele komplexe Herausforderungen. Datenanwendungen können helfen, diese Komplexität zu reduzieren und neue Chancen zu nutzen. Ein rein technischer Ansatz wird dabei aber scheitern, ein rein qualitativer Ansatz ebenfalls. Für den verantwortungsvollen und wirkungsorientierten Umgang mit datenbasierten Systemen und daraus abgeleiteten maschinellen Entscheidungen im öffentlichen und sozialen Sektor brauchen wir ein sozialwissenschaftliches Verständnis der Daten und der Methoden der Datenwissenschaften. ●

Johannes Müller ist Data Scientist und Sozialwissenschaftler. Er ist Mitgründer und Chief Data Scientist bei der Datenberatung cause&effect UG und Gründer und Vorsitzender von CorrelAid e.V. Er hält einen Master of Science in „Evidence-based Social Intervention and Policy Evaluation" von der University of Oxford.



KRISENMANAGEMENT UND CYBER-BEDROHUNGEN

Informationssicherheit und Informationssicherheits-Management in Zeiten der Pandemie

| von MORITZ HUBER und JENS WESTPHAL

Die Corona-Krise hat das gesellschaftliche Leben in Deutschland und weltweit in einer Art und Weise verändert, wie es sich nur die Wenigsten hätten vorstellen können. Innerhalb kürzester Zeit haben Gesellschaft, Wirtschaft und öffentliche Einrichtungen ihr Zusammenleben und -arbeiten neu organisiert. Unternehmen und Behörden haben kreativ und pragmatisch Lösungen für immer neue Herausforderungen gefunden. Jetzt ist es an der Zeit zu konsolidieren und zu optimieren. Denn die in Rekordzeit implementierten Systeme und Prozesse werden Grundlage für weitere Maßnahmen im Umgang mit der Krise sein.

COVID-19: KATALYSATOR DES DIGITALEN WANDELS

Zumindest in einem Punkt scheint das Virus auch einen positiven Effekt zu haben: COVID-19 wirkt als eine Art Katalysator für verschiedenste Digitalisierungsprozesse und das höchstwahrscheinlich über das noch nicht absehbare Ende der Krise hinaus. Es hat zur Verlagerung von vielen Arbeitsplätzen ins Homeoffice geführt. Die Beantragung der kurzfristig beschlossenen Soforthilfemaßnahmen für Unternehmen ist über eilig eingerichtete Internetplattformen erfolgt. Und zur Identifizierung und Unterbrechung von Infektionsketten wurde eine Tracing-App für Smartphones entwickelt.

Die genannten Beispiele haben zwei Gemeinsamkeiten: Zum einen basieren sie auf moderner Informations- und Kommunikationstechnik. Zum anderen wurden die bereits implementierten Systeme und Prozesse unter Hochdruck extrem schnell entwickelt und mit der sprichwörtlichen „heißen Nadel" gestrickt. Dieser Umstand birgt einige Risiken.

KRISENBEWÄLTIGUNG AUF KOSTEN DER SICHERHEIT

Die Bedrohungslage durch Cyberangriffe hat sich deutlich verschärft. Am Beispiel der großflächigen Einrichtung von Homeoffice-Arbeitsplätzen wird die Problematik besonders deutlich. Behörden, die bislang Remote-Zugriffe auf ihre IT-Systeme und Daten restriktiv gehandhabt haben, sind nun Risiken eingegangen, die unter anderen Umständen wohl niemals genehmigt worden wären: Die Nutzung privater Rechner zu dienstlichen Zwecken, Kommunikation über unverschlüsselte Leitungen oder schwach abgesicherte Zugriffsverfahren an der Schnittstelle zwischen den Verwaltungsnetzen und dem Internet sind nur einige besonders kritische Schwachstellen. Und dieser gestiegenen Verwundbarkeit der öffentlichen IT-Systeme stehen global agierende Cyberkriminelle und nachrichtendienstliche Akteure gegenüber. Erste Betrugsversuche sind bekannt geworden und rufen Schlagzeilen der Vor-Corona-Zeit in Erinnerung: Bei den Cyberangriffen auf das Klinikum Neuss[1], das Kammergericht in Berlin[2] oder die Universität Gießen[3] kam es zu langwierigen Systemausfällen und enormen Schäden. Ganz aktuell ist der Angriff auf die Technischen Werke Ludwigshafen[4], bei dem im großen Stil auf Geschäfts- und Kundendaten zugegriffen werden konnte.

UNSICHERE SYSTEME TREFFEN AUF SKRUPELLOSE TÄTER

Dass Hacker und Cyberkriminelle bereit sind, diese neuen Schwachstellen auszunutzen, betonen die Lageberichte der Sicherheitsbehörden. EUROPOL kommt beispielsweise zu dem Ergebnis, dass die Auswirkungen von COVID-19 in keinem anderen Kriminalitätsfeld so spürbar sind wie im Cyberbereich.[5]

Neue Verschlüsselungstrojaner, Phishing-Kampagnen und eine Neuausrichtung der Underground-Economy sind Schattenseiten der Digitalisierung. Die Folge sind Schäden aufgrund krimineller Cyberangriffe, die unter Umständen ganze Behörden lahmlegen und deren Beseitigung dann viel Zeit und Geld kostet. Was also tun?

DIGITALISIERUNG BRAUCHT EINE SUBSTANZIELLE RISIKOANALYSE

Nur digital gestützte Prozesse ermöglichen es, die in der Krise erforderliche Reaktionsgeschwindigkeit zu erreichen, etwa bei der Nachverfolgung von Infektionsketten bei Pandemien und der Benachrichtigung von Betroffenen. Darum ist eine schnelle Digitalisierung notwendig. In der Praxis wird alles, was dabei hinderlich sein könnte, zunächst zur Seite geschoben. So wird zum Beispiel die Absicherung der eilig aus dem Boden gestampften digitalen Prozesse mit Mitteln der Informationssicherheit gerne als ein solches bremsendes Element wahrgenommen – und deshalb vernachlässigt. Die dadurch entstandene mangelhafte Sicherheit bleibt dann langfristig erhalten und stellt permanent Einfallstore für Angreifer bereit.

Wenn digital gestützte Prozesse entstehen, an bestehenden Systemen Veränderungen vorgenommen oder neue Systeme entwickelt werden, müssen zunächst die dabei neu oder zusätzlich entstehenden Risiken identifiziert und zumindest sehr zeitnah gezielt behandelt werden. Das ist eine Aufgabe für erfahrene Spezialisten, die um die Bedrohungsszenarien wissen, sämtliche Schwachstellen erkennen und in einem dynamischen Prozess die richtigen Schlussfolgerungen ziehen. Externe Experten aus spezialisierten Beratungshäusern, Organisationen, CERTs oder Ähnlichem überblicken die technischen und organisatorischen Folgen, können sie einordnen und bewerten und den Prozess bis zur Implementierung eines Informationssicherheits-Managementsystems (ISMS) begleiten.

BASIS GANZHEITLICHER SCHUTZMASSNAHMEN IST EIN MASSGESCHNEIDERTES ISMS

Bereits kurz nach der Jahrtausendwende hatte die Bundesverwaltung erkannt, dass den (damals noch) neuartigen Gefahren aus dem Cyberraum adäquat begegnet werden muss. Ab 2005 wurde dann der Nationale Plan zum Schutz der Informationsinfrastrukturen (NPSI) formuliert, der mit dem Umsetzungsplan (UP) Bund 2007 konkretisiert wurde. Im Juli 2017 hat das Bundeskabinett eine Neufassung des UP Bund beschlossen. Dies ist die heute gültige Leitlinie zur IT-Sicherheit in der Bundesverwal-

tung.[6] Der UP Bund setzt verbindliche Rahmenbedingungen für den Schutz der in der Bundesverwaltung verarbeiteten Informationen und der dazu genutzten Systeme, Dienste und Infrastrukturen. Er verpflichtet die Behörden zu einem nachhaltigen und standardisierten Informationssicherheitsmanagement (ISMS) und zur Sicherstellung eines angemessenen Sicherheitsniveaus. Solche ISMS sind heute in der Bundesverwaltung noch nicht überall vorhanden beziehungsweise wirksam. Institutionen jedoch, die über ein funktionsfähiges ISMS verfügen, das zudem auf die jeweils spezifischen Belange zugeschnitten ist, sind bei gleichbleibend hohem Sicherheitsniveau schneller in der Reaktion und Anpassung als Häuser ohne ISMS.

AUCH DYNAMISCHE PROZESSE UND AGILE ENTWICKLUNGEN KÖNNEN SICHER GESTALTET WERDEN

Ein wesentliches Merkmal eines ISMS ist seine Fähigkeit zur Erneuerung und Berücksichtigung von Entwicklungen, die beim ursprünglichen Aufbau dieses ISMS noch nicht abzusehen waren. Dafür ist es von Zeit zu Zeit erforderlich, die grundlegenden Paradigmen des ISMS zu überprüfen. Dies gilt insbesondere jetzt in der Krise: Die im Einsatz befindlichen ISMS müssen unter Berücksichtigung der veränderten Bedrohungslage nachjustiert werden. Das beinhaltet etwa organisationsspezifische Maßnahmen, die eine dynamische Reaktion auf krisenartige Entwicklungen ermöglichen. Beispielsweise kann der Aufbau von Krisenreaktionsteams (auch organisationsübergreifend) oder das Vorhalten von Equipment für sicheres Remote-Arbeiten erforderlich sein. Zumindest müssen Pläne erstellt und geprobt werden, um in der Krise die Verfügbarkeit operativer Prozesse zu erhalten oder schnell wiederherzustellen.

Doch auch jenseits der Krise sind Anpassungen möglich und nötig. So wurden in der Bundesverwaltung in den letzten Jahren in Ergänzung zum klassischen V-Modell XT auch agile Entwicklungsumgebungen geschaffen. Ein darauf zugeschnittenes ISMS kann Einfluss auf die Sprints agiler Projekte nehmen und diese gegebenenfalls verhindern, wenn die IT-Sicherheit eines Inkrements (zu weit) von den Anforderungen abweicht. Im Ergebnis können sich Fehler in konzeptionellen Vorgaben oder deren Umsetzung gar nicht erst einschleichen. Damit sind auch für agile Prozesse in der Softwareentwicklung die Regeln auf Grundlage des ISO-Standards 27034-3 (Application Security Management Process) umgesetzt.

RISIKOBEGRENZUNG DURCH KOSTEN-NUTZEN-ANALYSE

Empfehlenswert ist ein standardisiertes Vorgehen zum Umgang mit Risiken, das sich an der ISO 31000 orientiert, dabei aber die für schnelle Reaktionen notwendigen Abkürzungen innerhalb der Norm nimmt. Die ISO 31000 legt Wert auf Vollständigkeit, lässt aber auch Freiräume in der Ausgestaltung und Umsetzung. Darüber hinaus ist es möglich, den Risikomanagementprozess an andere bestehende Managementsysteme anzulehnen und damit von Erkenntnissen zu profitieren, die in der Organisation bereits vorhanden sind. Der ganzheitliche Ansatz betrachtet IT-Risiken nicht isoliert, wie es beispielsweise bei einem Vorgehen nach ISO 27005 oder BSI 200-3 geschieht. Vielmehr werden generalisierte unternehmerische Risiken, die innerhalb der IT wirksam werden, in der Gesamtsicht bewertet und quantifiziert. Auf diese Weise werden Risiken minimiert, ohne dass der dafür betriebene Aufwand (zeitlich und finanziell) den angestrebten Nutzen übersteigt. ●

Moritz Huber beschäftigt sich als Kriminalbeamter, Wirtschaftsinformatiker und Dozent schon viele Jahre mit dem Thema Sicherheit aus unterschiedlichen Perspektiven. Derzeit leitet er die Zentrale Ansprechstelle Cybercrime (ZAC) im Landeskriminalamt Baden-Württemberg und promoviert zudem am „The Open Government Institute (TOGI)" der Zeppelin Universität im Themenfeld „Smart Security".

1 https://www.kma-online.de/aktuelles/klinik-news/detail/900000-euro-gesamtschaden-durch-cyberattacke-a-31629 (abgerufen am 15.07.2020).
2 https://www.tagesspiegel.de/berlin/cyberangriff-auf-berliner-kammergericht-russische-hacker-koennten-justizdaten-gestohlen-haben/25477570.html (abgerufen am 15.07.2020).
3 https://www.forschung-und-lehre.de/politik/uni-giessen-nach-cyberangriff-groesstenteils-wieder-online-2652/ (abgerufen am 15.07.2020).
4 https://www.ludwigshafen24.de/ludwigshafen/ludwigshafen-hacker-twl-deutschland-angriff-technische-werke-strom-kunden-daten-passwort-gefahr-13748874.html (abgerufen am 15.07.2020).
5 https://www.bild.de/news/ausland/news-ausland/wegen-corona-europol-warnt-cybercrime-betrug-und-diebstahl-nehmen-zu-69658798.bild.html (abgerufen am 15.07.2020).
6 https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html (abgerufen am 15.07.2020).

„KEIN ALLTÄGLICHES PROJEKT“

Drei Fragen an Dr. Holger Schmidt, Projektmanager für das RKI im Corona-Warn-App-Projekt

Es ist wohl das derzeit spannendste und meistdiskutierte Behördenprojekt: die Entwicklung der Corona-Warn-App. Dr. Holger Schmidt war als msg-Projektmanager für das RKI mittendrin. Er berichtet über die Herausforderungen und die intensive und sinnstiftende Arbeit an dieser App.

msg: Die Realisierung der Corona-Warn-App ist kein alltägliches Projekt – die gesellschaftliche Relevanz geht über das übliche Maß hinaus. Was waren die größten Herausforderungen?

Dr. H. Schmidt: Die größten Herausforderungen waren sicherlich der enorme Zeitdruck und die schiere politische Brisanz. Und ganz klar: das Wissen, dass es schlicht keine größeren Verzögerungen geben darf. Entsprechend war das Projekt einerseits natürlich sehr zeitintensiv – so etwas hatte ich bisher noch nicht! Wir haben von frühmorgens bis spätabends intensiv gearbeitet, auch an allen Wochenenden und Feiertagen. Teilweise hatten wir um 22:00 Uhr noch Telkos. Andererseits war es besonders schön zu sehen, wie groß das Commitment aller Beteiligten war, über alle Organisationen und vor allem auch alle Hierarchieebenen hinweg. Alle haben immer sehr lösungsfokussiert gearbeitet. Es ging nie darum, die Probleme herauszupicken. Immer gab es einen Zug in Richtung Lösung. Das war wahnsinnig motivierend.

msg: Die App stößt auf eine erfreulich hohe und positive Resonanz – auch bezüglich der IT-Sicherheit. Wie sicher ist die App denn?

Dr. H. Schmidt: Datenschutz und Sicherheit – und übrigens auch Barrierefreiheit – waren Themen, die von Anfang an sehr ernst genommen wurden. Das steht nicht in jedem Projekt im Vordergrund. Aus meiner Sicht hat dies dazu beigetragen, dass eine überaus datensparsame und sichere App entwickelt wurde. Hinzu kommt natürlich der Open-Source-Gedanke. Da das Ganze frühzeitig Open Source gestellt wurde, hat sich schnell eine Community gebildet. Findige Leute haben sich das genau angeschaut, teilweise auch Sicherheitslücken entdeckt und entsprechend gemeldet. Das wurde von Anfang an berücksichtigt und gleich behoben. Noch mal: Ich denke, dass man schon guten Gewissens sagen kann, alle Beteiligten habe eine sichere und datensparsame App entwickelt.

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BFDI) wurden ebenfalls frühzeitig einbezogen. Und selbst der Chaos Computer Club (CCC) lobt die App. Wir sehen gerade, wie positiv die Berichterstattung ist. Das wäre sie sicherlich nicht, wenn es tatsächlich gravierende Probleme gäbe. Das Projekt hat so eine außergewöhnliche Sichtbarkeit und Schlagkraft. In normalen Zeiten hätte ein solches Projekt vermutlich viele Monate, vielleicht sogar Jahre gebraucht.

msg: Sicherlich ein gutes Gefühl, einen Beitrag für so ein besonderes Projekt geleistet zu haben, oder?

Dr. H. Schmidt: Definitiv. Es ist schon besonders motivierend, wenn man den Sinn des Projektes so unmittelbar sieht und spürt. In dieser Form ist das nicht immer gegeben. Einfach schön. Auch so direkt am Puls der Zeit zu sein. Positiv bleibt mir auch in Erinnerung, dass die Arbeit zum großen Teil via Videokonferenzen stattgefunden und dabei so erfolgreich funktioniert hat. Teilweise waren wir den ganzen Tag in Videokonferenzen mit SAP, der Telekom, den Ministerien, mit dem PMO auf der Telekom-/SAP-Seite. Das hat richtig gut geklappt und über diese Intensität haben wir auch eine sehr gute Beziehung zu den anderen Projektbeteiligten aufgebaut.

Das vollständige Interview finden Sie im Newsroom der msg (https://www.msg.group/standpunkt).

Organisationen versuchen ständig, neue Wege zu finden, um die an sie gestellten Herausforderungen in ihrer täglichen Arbeit effektiv und effizient zu lösen. Herausforderungen sind zum Beispiel, neue Produkte und Dienstleistungen zu entwickeln oder bestehende zu verbessern. In diesem Punkt unterscheidet sich die öffentliche Verwaltung nicht von anderen Branchen. Design Sprints als Methode sind dabei ein nützliches Handwerkszeug, um innerhalb eines sehr kurzen Zeitraums bestehende Herausforderungen zu identifizieren, Lösungen zu entwerfen und mit der Zielgruppe, das heißt in der öffentlichen Verwaltung meist mit dem Bürger, zu validieren.

| von **RALF MICHEL**

DESIGN SPRINTS – IN WENIGEN TAGEN VON DER HERAUSFORDERUNG ZUM BÜRGERFEEDBACK

WARUM DESIGN SPRINTS?

Heutzutage (in der sogenannten modernen oder auch VUCA[1]-Welt) reicht es nicht mehr, eine gute Idee zu haben. Es muss vielmehr „die" gute Idee sein. Design Sprints helfen dabei, viele Ideen zu entwickeln, die gute Idee zu finden und schnell zu erproben. Sie sind eine „von einem Moderator geführte, an bestimmte Zeitvorgaben gebundene feste Abfolge von Übungen, die ein interdisziplinäres Team zur fokussierten Lösung eines Problems mit hoher Geschwindigkeit durchläuft".[2] Der ursprüngliche Ansatz geht von einer Design-Sprint-Dauer von fünf Tagen aus. Aus heutiger Sicht und nach vielen Erfahrungen mit der Durchführung von Design Sprints ist es auch möglich, einen Design Sprint in vier Tagen oder in einem anderen gewählten Zeitrahmen durchzuführen. Hierbei ist jedoch zu beachten, dass der Design Sprint jeweils sorgfältig im Vorfeld geplant und vorbereitet werden muss.

WO UND WIE ENTSTAND DIE METHODE DER DESIGN SPRINTS?

Die Design-Sprint-Methode entstand um das Jahr 2010 bei Google Ventures, Googles eigener Risikokapitalgesellschaft. Hintergrund war die Herausforderung, einen kompletten Problemlösungszyklus zusammen mit Start-ups möglichst schnell, in diesem Fall innerhalb einer Woche, durchlaufen zu können. Verschiedene Teams innerhalb Google experimentierten damals schon mit verschiedenen Methoden, unter anderem mit unterschiedlichen Produktentwicklungsprozessen, wie zum Beispiel Scrum, Design Thinking[3] und einer Vielzahl von Elementen aus anderen Disziplinen, wie psychologischen und soziologischen Erkenntnissen rund um die Arbeitsweise von erfolgreichen Teams. Die wichtigsten Haupteinflüsse der späteren Design-Sprint-Methode werden im Detail in Abbildung 1 dargestellt. Das Ergebnis von Googles Anstrengung war es schließlich, dass den Teams eine Methode an die Hand gegeben werden konnte, um eindeutig definierte Ziele festzulegen, Annahmen zu validieren und ein Produkt oder eine Lösung in sehr kurzer Zeit auf Eignung zu prüfen, das heißt, bevor die eigentliche Umsetzung beginnt.[4]

WIE FUNKTIONIEREN DESIGN SPRINTS?

In die fünf Phasen des Design Sprints startet die ausführende Gruppe mit einer festgelegten Herausforderung. Aus dieser Herausforderung wird das Ziel des Design Sprints abgeleitet. Anschließend werden viele Ideen gesammelt (Stichwort: Kreativität und Divergenz in der Lösungsfindung), um diese in späteren Phasen zu analysieren, zu bewerten und auf einige wenige oder auch nur eine Idee zu verdichten (Stichwort: Konzentration auf eine beziehungsweise wenige Lösungen, die weiter ausgearbeitet werden – Konvergenz). Die in Abbildung 2 beschriebenen Phasen sind für ein erfolgreiches Gelingen eines Design Sprints notwendig. In diesem Artikel werden allerdings nicht nur die fünf bekannten Phasen aus einem Design Sprint mit fünf Tagen Dauer beschrieben, sondern auch die notwendigen Vor- und Nacharbeiten im Umfeld eines Design Sprints.

DIE VORBEREITUNG – WAS MUSS ALLES VOR DEM SPRINT GETAN WERDEN?

Bevor der Design Sprint starten kann, muss die passende und relevante Herausforderung festgelegt und das richtige Team mit den entsprechenden Fähigkeiten für die Lösungsfindung zusammengestellt werden. Diese Herausforderung kann am besten mit dem Entscheider herausgearbeitet werden, denn sie ist der Grund, weshalb der Design Sprint durchgeführt wird.

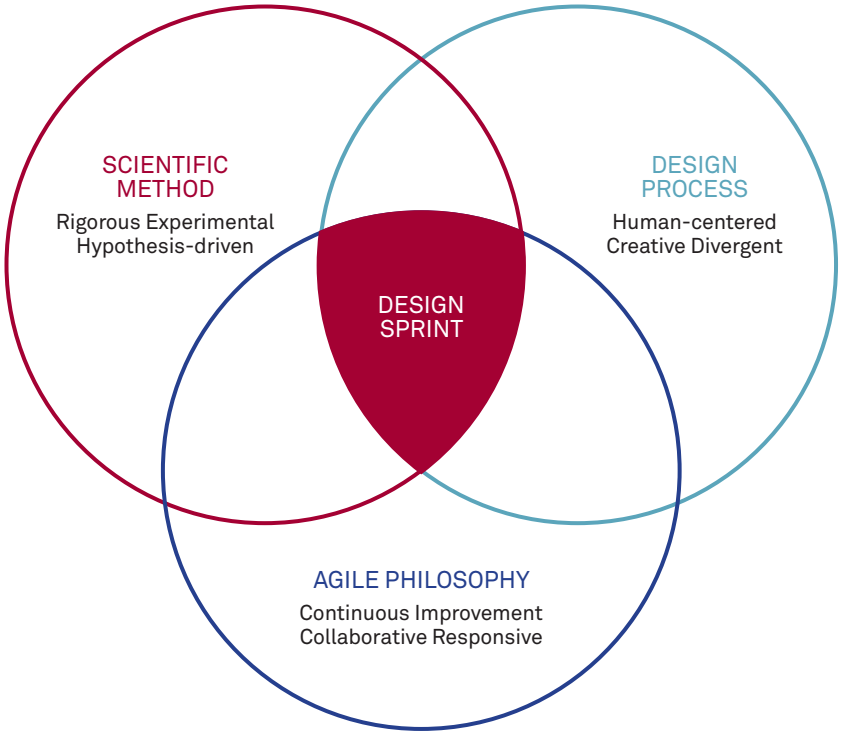


Abbildung 1: Haupteinflüsse der Design-Sprint-Methode

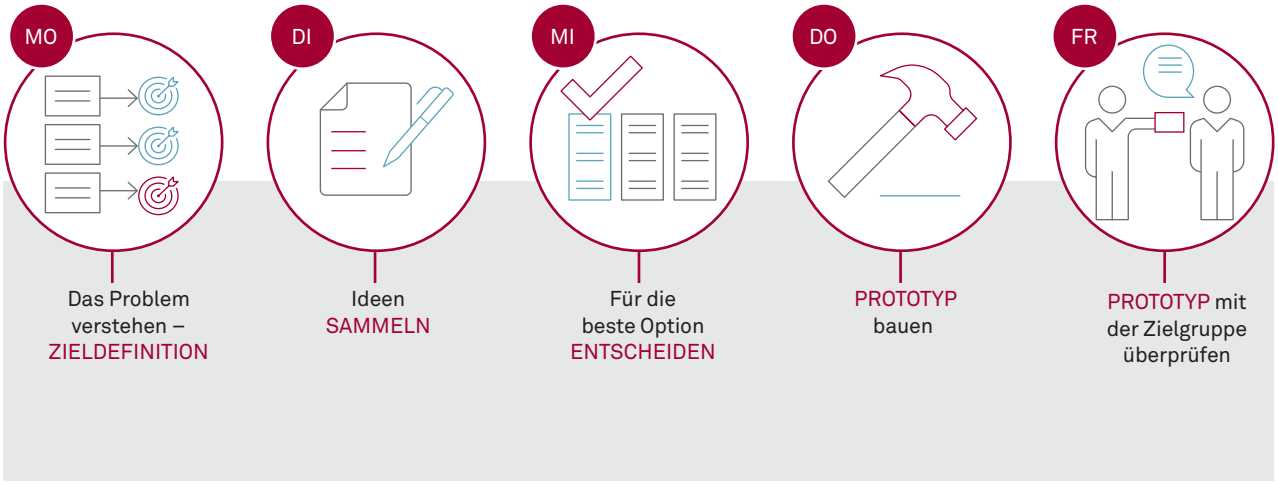


Abbildung 2: Phasen eines fünftägigen Design Sprints

Das Team umfasst idealerweise sieben Mitglieder mit unterschiedlichen Fähigkeiten und Hintergründen. Erfahrungsgemäß werden die besten Ergebnisse erzielt, wenn das Team fünf Tage ohne Unterbrechung am Design Sprint arbeiten kann. Das bedeutet, dass die einzelnen Experten von ihren täglichen Aufgaben freigestellt sind, um sich auf den Design Sprint konzentrieren zu können. Wichtig ist, dass auch (mindestens) ein Entscheider teilnimmt, da im Design Sprint viele Richtungsweisungen durch ihn getroffen werden müssen. Eine Vertretung des Entscheiders durch eine andere Person sollte aus Erfahrung, aufgrund der potenziell fehlenden Nachhaltigkeit der Entscheidungen, vermieden werden.

Der verwendete Raum muss für den Design Sprint mit allem nötigen Equipment, wie zum Beispiel Whiteboards, Flipcharts, Post-its, Stoppuhren, Stiften, Kameras (zur Dokumentation der Ergebnisse), Laptops, Druckern usw., ausgestattet sein. Auch muss schon früh abgestimmt werden, welche Experten an den Lightning Talks am ersten Tag des Sprints teilnehmen können. Die Aufgabe der Lightning Talks ist es, in Phase 1 das schon vorhandene Wissen von innerhalb oder außerhalb der Organisation im Rahmen von kurzen Vorträgen in den Design Sprint einzubringen.

Ganz wichtig schon in der Vorbereitung: Man muss sich um die Vertreter der Nutzergruppe, die an Tag 5 des Design Sprints als Interviewpartner zur Verfügung stehen müssen, kümmern. Aus Sicht der Schöpfer der Design-Sprint-Methode sind mindestens fünf Vertreter notwendig, um eine qualifizierte Aussage zur Anwendbarkeit der Lösungsidee zu bekommen.

Zu guter Letzt benötigt man für den Workshop einen Moderator, auch „Sprint Master“ oder „Design Sprint Master“ genannt, der die Diskussionen leitet, den jeweiligen Zeitrahmen für die Aufgaben festlegt und die Einhaltung der Design-Sprint-Methode steuert. Der Moderator für den Design Sprint ist in seiner Rolle immer neutral. Er kümmert sich voll und ganz um die Durchführung des Design Sprints.

Die Erfahrung zeigt, dass ungefähr zwei bis drei Wochen Vorbereitungszeit eingeplant werden müssen, um einen Design Sprint vorzubereiten, abhängig davon, wie sehr sich die verantwortliche Person neben ihrem Tagesgeschäft auf die Vorbereitung des Design Sprints konzentrieren kann.

PHASE 1 – MONTAG: DAS PROBLEM VERSTEHEN – ZIELDEFINITION

Aufgabe des ersten Tages (Montag) ist es, ausgehend von der Herausforderung ein Ziel zu definieren, das im Design Sprint, also innerhalb der festgelegten Zeit, erreicht werden soll. Dazu wird zuerst die vom Moderator in der Vorbereitung mit dem Entscheider ausgearbeitete Herausforderung vorgestellt. Im besten Fall macht dies der Entscheider (der meist auch der Auftraggeber des Design Sprints ist) auch selbst.

Im nächsten Schritt wird ein Langzeitziel festgelegt. Dazu müssen folgende Fragen beantwortet werden:

1. Wie entwickelt sich das Projekt oder das Produkt über die nächsten sechs bis zwölf Monate (oder auch länger), wenn alles positiv läuft (Optimismus – der sogenannte „Happy Path")?
2. Welche Annahmen und Risiken können die Zielerreichung beeinflussen (Pessimismus)? Diese Punkte werden zu Fragen, die unter anderem im Verlauf des Design Sprints beantwortet werden sollen.

Beide Aufgaben werden von den Teammitgliedern jeweils eigenständig ausgearbeitet, das heißt, jedes Teammitglied legt fest, wie Erfolg und Misserfolg für sie oder ihn aussehen würden und wie es selbst das Langzeitziell formulieren würde.

Aus den Vorschlägen der Teammitglieder für das Langzeitziel (Dokumentation für alle sichtbar an einer Wand) wählt das Team eine Formulierung aus. Die Auswahl erfolgt mithilfe von Klebepunkten, das heißt, jeder Teilnehmer der Gruppe hat einen Punkt zu vergeben. Die Wahl des Teams ist allerdings nicht bindend, denn letztendlich wählt der Entscheider die aus seiner Sicht passende Formulierung aus. Das Langzeitziel wird dem gesamten Team helfen, während des Sprints die Frage nach dem „Warum" zu beantworten. Im nächsten Schritt wird eine Darstellung der Herausforderung erzeugt. Meist wird hierzu eine Customer-Journey-Map, die das Kundenerlebnis und die Kundenbeziehung beschreibt, verwendet. Eine Customer Journey Map ist eine visuelle Darstellung aller Begegnungen und Interaktionen der Akteure der Zielgruppe mit der Organisation als Ganzes. Anhand dieser Reise der Akteure entlang der Interaktion mit der Organisation lassen sich die weiteren Fragestellungen bearbeiten. Als Nächstes können am ersten Tag des Sprints kurze Expertenbefragungen (maximal 5 bis 15 Minuten), die sogenannten Lightning Talks, stattfinden. Parallel zu den Lightning Talks und danach werden vom Team „Wie-können-wir-Fragen" erstellt und an einer Wand dokumentiert (inklusive Clustering). „Wie-können-wir-Fragen" sind Hindernisse, die als Herausforderungen beschrieben sind. Anhand der Antworten auf diese Fragen kann erfasst werden, wie man die Interaktion mit der Zielgruppe verbessern beziehungsweise aufbauen kann.

Als letzter Schritt wird das Ziel des Design Sprints festgelegt, indem die für den Sprint relevanten „Wie-können-wir-Fragen", dokumentiert an einer Wand, ausgewählt werden (zwei Klebepunkte für die Teammitglieder und vier für den Entscheider). Der Entscheider sucht unter Verwendung seiner Klebepunkte die vier „Wie-können-wir-Fragen" aus, die er am interessantesten und am wichtigsten findet. Die Beantwortung dieser vier ausgewählten Fragen stellt schlussendlich das Ziel des gesamten Design Sprints dar.

Der erste Tag ist eine der anspruchsvollsten und anstrengendsten Phasen des Design Sprints, da das Team – um den Sprint erfolgreich durchführen zu können – vor der Herausforderung steht, das langfristige Ziel und das Ziel des Design Sprints zum Teil auszuarbeiten und zu verstehen. Der Moderator muss gerade an diesem Tag besonders darauf achten, das Team mitzunehmen und nicht zu überfordern.

PHASE 2 – DIENSTAG: IDEEN SAMMELN

Gute Ideen sind nicht einfach zu finden. Um dies zu schaffen, ist erst einmal eine große Anzahl an Ideen nötig (Divergenz in der Ideenfindung). Der Dienstag steht daher im Zeichen des Ideensammelns. Der Fokus der Teilnehmer ändert sich von „Verstehen" zu „Lösen". Dazu arbeitet jedes Gruppenmitglied selbstständig eine eigene Lösungsidee im Detail aus. Um das volle schöpferische Potenzial der Gruppe zu heben, unterstützt sie der Moderator dabei mit unterschiedlichen Kreativitätstechniken. Es ist in der Suche nach Ideen explizit erwünscht, auch über den eigenen Tellerrand hinauszublicken („Wie haben andere das gleiche Problem oder ähnliche Probleme gelöst?").

Am Ende des Tages muss jedes Mitglied des Teams in der Lage sein, seine Idee anhand einer Skizze der Gruppe zu präsentieren. Wie die Präsentation im Detail aussieht, ist jedem Teilnehmer selbst überlassen. Aus der Erfahrung zeigt sich, dass die Skizzierung auf Papier am sinnvollsten ist. Die eigentliche Präsentation der Lösungsideen ist jedoch für den nächsten Tag vorgesehen.

PHASE 3 – MITTWOCH: ENTSCHEIDEN

Nun kommt es zur Konvergenz in der Lösungsfindung, das heißt, die Anzahl der potenziellen Lösungsideen wird verringert. Am Mittwoch werden dazu alle Lösungen besprochen und in der Gruppe bewertet. Generell werden sie in diesem Schritt nicht nach richtig oder falsch bewertet, sondern danach, ob sie mehr oder weniger geeignet sind, einen Weg zu ebnen, um das Problem zu lösen. Nach der Vorstellung der Lösungen wählt der Entscheider aus, welche Lösungsidee oder -ideen (generell sind immer auch mehrere Lösungsideen und Prototypen möglich) weiterhin betrachtet werden sollen. Dabei bezieht er stets auch die Meinung des Teams in die Entscheidung ein.

Damit die Entscheidung nicht zu einer langen Diskussion wird, empfiehlt die Design-Sprint-Methode die Verwendung der sogenannten „Sticky Decision". Das bedeutet, dass alle Lösungsskizzen im Raum sichtbar aufgehängt werden (Skiz-

zengalerie). Danach betrachtet jedes Gruppenmitglied die Lösungsskizzen und vergibt ein bis drei Klebepunkte. Durch diese Kleberunde soll die Tendenz erkennbar werden, und die Aufmerksamket der Teammitglieder sich auf die Skizzen mit den meisten Punkten richten (dieses Vorgehen wird im Design-Sprint-Kontext „Heat Map" genannt). Ist dies abgeschlossen, findet eine dreiminütige (wichtig: Timeboxing durch den Moderator) Auseinandersetzung mit den Lösungsskizzen statt, in der noch offene Fragen des Teams vom Ersteller der jeweiligen Skizze beantwortet werden können. Nachdem alle Lösungsskizzen vorgestellt wurden, muss jedes Gruppenmitglied seine bevorzugte Lösung mit einem Klebepunkt markieren. Das letzte Wort hat wieder der Entscheider. Er legt schlussendlich fest, welche Lösungsskizze als Prototyp ausgearbeitet wird. Der Entscheider erhält für diesen Schrittt drei Klebepunkte: Mit einem wählt er seine favorisierte Lösungsskizze aus. Mit den beiden anderen kann er zusätzliche Features aus den verworfenen Lösungsskizzen hinzuwählen.
In der zweiten Hälfte des Tages wird ein Storyboard für den Prototyp erstellt. Dazu muss sich das Team in die Interviewsituation am letzten Tag hineinversetzen. Das Storyboard an sich ist eine Art Drehbuch, das beschreibt, wie die Abläufe im Rahmen des Prototyps aussehen werden. Meist wird für die Erstellung des Storyboards eine Papierwand mit 15 Kästchen verwendet. Jedes Kästchen beschreibt visuell einen Schritt des Prototyps. Anhand dieses erstellten Storyboards wird dann am folgenden Tag der Prototyp realisiert.

PHASE 4 – DONNERSTAG: PROTOTYP BAUEN IN EINEM TAG

In dieser Phase wird der Prototyp für die Lösungsidee gebaut – allerdings kein realer Prototyp, sondern eine Art Simulation (eine sogenannte Fassade) für den Test der Lösungsidee mit der Zielgruppe. Dabei konzentriert man sich zum Beispiel auf das User Interface des Prototyps, mit dem die Zielgruppe interagiert. Es können alle vorhandenen Materialien verwendet und zudem kurzfristig weitere Materialien beschafft werden. Meist wird der Prototyp aus Papier erstellt, aber auch andere Arten sind möglich. Die Erstellung erfolgt gemeinsam im Team, wobei jedes Teammitglied eine Aufgabe übernimmt, zu der es am meisten beitragen kann. Manche Teams sind sogar in der Lage, ein digitales Mock-up (Vorführmodell) als Prototyp zu erstellen.

Wichtig sind in dieser Phase wenige teaminterne Überprüfungen, um sicherzustellen, dass die später zu testenden Hypothesen und die vorhandenen offenen Fragen an die Zielgruppe im Blick des Teams bei der Prototyperstellung bleiben. Neben der Prototyperstellung gehört in das Arbeitspaket des Donnerstags auch die Erstellung eines Zeitplans für den Nutzertest mit der Zielgruppe am Freitag und die Erstellung eines Interviewleitfadens. Mit dem Interviewleitfaden soll sichergestellt werden, dass an Tag 5 die relevanten und wichtigen Fragen gestellt werden, um der Problemlösung einen Schritt näher zu kommen.

PHASE 5 – PROTOTYP MIT DER ZIELGRUPPE ÜBERPRÜFEN

Der Freitag ist die Essenz des Design Sprints. Bis zu diesem Tag wurden Lösungsideen entwickelt, eine Idee wurde ausgewählt und ein Prototyp für die Validierung mit der Zielgruppe gebaut.

Nun kommen die Vertreter der Zielgruppe ins Spiel. Ziel ist es, den Prototyp ungefähr fünf Vertretern der Nutzergruppe vorzustellen und anschließend die vorbereiteten Feedbackinterviews zu führen. Vorrangig ist dabei, zu erfahren, wie die Zielgruppenvertreter mit dem Prototyp umgehen und welche Reaktionen bei den Interviewten auftreten. Mehrere Vertreter aus der Zielgruppe zu interviewen, erlaubt, Muster in der Nutzung zu erkennen und festzustellen, welche Aspekte des Prototyps die Anforderungen und Erwartungen der Zielgruppe erfüllen und welche Eigenschaften des Prototyps durchfallen. Gleichzeitig kann das Team von den Interviewten Antworten auf seine offenen Fragen aus der Phase der Prototyperstellung erhalten.

Am Ende des fünften Tags werden die Erkenntnisse aus den Interviews im Team vorgestellt und beispielsweise per Klebezettel an einer Wand dokumentiert. Die Erkenntnisse können dabei jeweils positiv, negativ oder neutral sein. Bei der Aufnahme der Erkenntnisse ist es die Aufgabe des Moderators, dafür zu sorgen, dass es nicht zu intensiven Diskussionen kommt, die sehr viel Zeit kosten können. Schlussendlich wird der Entscheider befragt, ob das Team mit seiner Lösungsidee und mit seinem Prototyp dabei geholfen hat, die Organisation bei der Beantwortung der anfänglichen Fragestellung weiterzubringen. Eine Dokumentation der Ergebnisse zur weiteren Verwendung in der Organisation ist obligatorisch.

WAS GESCHIEHT NACH DEM DESIGN SPRINT?

Nach dem Design Sprint ist es essenziell, das Momentum nicht zu verlieren. Denn zu keiner anderen Zeit als nach dem Design Sprint ist das Team enthusiastischer und möchte auch den nächsten Schritt gehen. Das bedeutet, dass das Team die Erwartung hat, die erarbeiteten Ergebnisse aus dem Design Sprint in eine Umsetzung zu übernehmen. Wichtige Aufgabe ist zunächst, die Ergebnisse bei den

jeweiligen Stakeholdern in der Organisation oder auch gegebenenfalls außerhalb vorzustellen. Denn bisher sind die Ergebnisse nur der kleinen Gruppe aus dem Design Sprint bekannt. Parallel dazu können weitere Design Sprints durchgeführt werden, um weitere Fragestellungen zu lösen. Schlussendlich muss dann die Umsetzung der Ergebnisse in der Realität, zum Beispiel durch ein Produkt, eine Dienstleistung oder eine Optimierung der bestehenden Verhältnisse, erfolgen.

DESIGN SPRINTS IN DER ÖFFENTLICHEN VERWALTUNG – WO WERDEN SIE HEUTE EINGESETZT?

Design Sprints werden heute überall eingesetzt. Sie sind von einer Methode, die nur von Google genutzt wurde, zu einer bekannten und weitverbreiteten Methode zum Finden von Lösungen und Innovationen geworden. Es existieren viele Erfolgsgeschichten aus der Industrie und der öffentlichen Verwaltung, die auch im Internet zu finden sind.[5]

In der öffentlichen Verwaltung werden Design Sprints häufig im Zusammenhang mit der Digitalisierung von Verwaltungsleistungen im Rahmen des Onlinezugangsgesetzes (OZG)[6] eingesetzt. Das OZG verpflichtet Bund und Länder, bis spätestens 2022 ihre Verwaltungsleistungen den Bürgern und Unternehmen auch elektronisch über Verwaltungsportale anzubieten. Damit soll einerseits der Aufbau eines Bundesportales, inklusive Nutzerkonto als Identifizierungskomponente, umgesetzt werden. Andererseits beinhaltet das Gesetz die Verknüpfung der Verwaltungsportale von Bund und Ländern zu einem Portalverbund, die Bereitstellung von Basisdiensten und IT-Komponenten sowie den vollständigen Ausbau digitaler Verwaltungsleistungen bis Ende 2022.

Für die nutzerfreundliche Digitalisierung von Verwaltungsleistungen werden in den OZG-Themenfeldern[7] Design Sprints eingesetzt, um die in einer Gruppe entwickelten Ideen mit den Bürgern in kurzer Zeit zu validieren und damit unter anderem Anforderungen für die IT-technische Umsetzung abzuleiten. Design Sprints wurden zum Beispiel in Sachsen-Anhalt eingesetzt, um im Digitalisierungslabor BAföG eine Vorgehensweise für die BAföG-Antragstellung zu entwickeln. Mithilfe von exemplarischen BAföG-Antragstellern wurden Lösungsideen entwickelt, überprüft und entweder verworfen oder in einem nachfolgenden Schritt weiterentwickelt. In Hessen wurden Design Sprints für die Bearbeitung der Schmerzpunkte der Bürger im Rahmen der Digitalisierung der Verwaltungsleistung „Antrag auf Ersterteilung der Fahrerlaubnis“ eingesetzt. In Berlin wurden Ideen für die Erstellung einer „Digitalen Geburtsurkunde“ gesucht und mit der Zielgruppe überprüft. Ideen für eine Online-Bürgerbeteiligung wurden in Schleswig-Holstein entwickelt und mit Bürgern validiert, und in Sachsen wurden Design Sprints für die Suche nach Lösungen bezüglich der Digitalisierung der Verwaltungsleistung „Verkehrs- und Ordnungswidrigkeiten“ (Bearbeitung von Bußgeldverfahren wegen Ordnungswidrigkeiten im Straßenverkehr) eingesetzt. Auch außerhalb Deutschlands gibt es positive Erfahrungen und Erfolgsmeldungen bezüglich Design Sprints. Sie werden im Rahmen der Digitalisierung von Verwaltungsleistungen in Großbritannien (GOV.UK) verwendet (zum Beispiel Ministry of Justice (MoJ), Department for Work and Pensions (DWP)). Auch in Estland haben Design Sprints dazu beigetragen, das Land an die Spitze der Digitalisierung in Europa zu bringen.

Zusammenfassend lässt sich sagen, dass der Einsatz von Design Sprints in Digitalisierungs- und Innovationslaboren an vielen Orten positiv aufgenommen wurde und sehr gute Ergebnisse damit erzielt wurden. Sie helfen dabei, Lösungsideen schnell und früh im Innovations- beziehungsweise Digitalisierungsprozess mit den späteren Nutzern, das heißt den Bürgern, zu überprüfen. Die Teilnehmer an den Design Sprints sind von der Methode häufig begeistert und wie die Auftraggeber mit den gemeinsam erarbeiteten Ergebnissen zufrieden. ●

1 VUCA: V = Volatility/Volatilität, U = Uncerntainty/Unsicherheit, C = Complexity/Komplexität, A = Ambiguity/Mehrdeutigkeit. Das Akronym beschreibt die schwierigen Rahmenbedingungen in der heutigen modernen Welt.
2 Aus: „Das Design Sprint Handbuch“ – J. Noack, J. Diaz, dpunkt.verlag, 2019.
3 .public 01/2017.
4 Internetauftritt von GV zu Design Sprints: https://www.gv.com/sprint/ (aufgerufen im Januar 2020).
5 Darstellung von Erfolgen mit Design Sprints: https://sprintstories.com/ (aufgerufen im Januar 2020).
6 Das Onlinezugangsgesetz: https://www.onlinezugangsgesetz.de/ (aufgerufen im Januar 2020).
7 OZG-Themenfelder: https://www.it-planungsrat.de/DE/ITPlanungsrat/OZG-Umsetzung/Digitalisierungsprogramm/04_DigPro_Themenfeldplanung/DigPro_Themenfeldplanung_node.html;jsessionid=2F0379409ABC52757D0E8A94EE4F1512.1_cid350 (aufgerufen Januar 2020).

AUTORENVERZEICHNIS

Dr. Katrin Ehlers ist promovierte Literatur- und Medienwissenschaftlerin. Sie verfügt über langjährige Erfahrung mit Kommunikationsaufgaben von Politik und Verwaltung, von Unternehmen und Institutionen im Gesundheitsbereich sowie aus anderen Branchen. Bei msg verantwortet sie das Marketing in der öffentlichen Verwaltung.

Dr. Roger Fischlin ist promovierter Diplom-Informatiker und -Mathematiker und berät bei der msg systems ag Kunden im Themenbereich IT-Management und insbesondere Informationssicherheit. Er verfügt über langjährige Erfahrungen im öffentlichen Sektor und in der Finanzbranche. Zudem ist er CISA, CISM, CRISC und CISSP sowie ISO 27001 Lead Auditor und Lehrbeauftragter für IT-Organisation an der Hochschule Pforzheim.

Jürgen Fritsche ist Geschäftsleiter des msg systems Public Sectors sowie Mitglied der Geschäftsleitung der msg systems ag. Er hat langjährige Erfahrung im Aufbau und in der Führung von Beratungs- und Systemintegrationseinheiten sowie im Management von Beratungsmandaten und Entwicklungsprojekten. Außerdem ist er Autor von Fachartikeln und erfahrener Referent zu Digitalisierungsthemen.

Dr. Atila Kaya ist promovierter Informatiker und für die msg systems ag als Lead IT-Architect in der öffentlichen Verwaltung tätig. Er verfügt über langjährige Erfahrung in der Implementierung komplexer verteilter Unternehmensanwendungen, in IT-Architektur und in der technischen Projektleitung.

Laszlo Lück ist bei der msg systems ag als Lead IT Consultant im Public Sector tätig. Er verfügt über langjährige Erfahrung beim Aufbau von mikroserviceorientierten Architekturen, bei der Entwicklung von IT-Software mit funktionalen Programmiersprachen, beim Entwurf von komplexen IT-Systemen mit modernen Bestandteilen wie Apache Kafka, Apache Cassandra, Elasticsearch, Docker.

Ralf Michel ist Diplom-Informatiker und für die msg systems ag als Lead Projekt Manager in der öffentlichen Verwaltung tätig. Seine Schwerpunkte sind agile Methoden und das klassische Projektmanagement. Während seiner langjährigen Tätigkeit hat er in der öffentlichen Verwaltung und in weiteren Branchen Kunden beraten und IT-Projekte geleitet.

Ludwig Scherr ist Diplom-Betriebswirt (FH) und bei der msg systems ag als Principal Project Manager in der öffentlichen Verwaltung tätig. Seine Expertise liegt im Application-Lifecycle-Management sowie im IT-Service-Management. Er hat weitreichende Erfahrung im gesamten Lifecycle von Entwicklung bis Betrieb von IT-Lösungen, sowohl im klassischen als auch im agilen Umfeld.

Dr. Holger Schmidt ist promovierter Informatiker und als Abteilungsleiter bei der msg systems ag in Nürnberg tätig. Er verfügt über langjährige Projekterfahrung im agilen und klassischen Projektmanagement und beschäftigt sich intensiv mit dem Thema Kanban zur Steuerung von IT-Projekten.

Jens Westphal verantwortet als Bereichsleiter das Thema Informationssicherheit im Public Sector und für kritische Infrastrukturen bei msg. Er verfügt über mehr als 20 Jahre branchenübergreifende Erfahrungen in der Beratung von Organisationen und ist ausgewiesener Spezialist für Aufbau und Betrieb von Informationssicherheitsmanagementsystemen nach ISO 27001 oder IT-Grundschutz.

IHNEN GEFÄLLT DIE AUSGABE? DANN ABONNIEREN SIE .public UND EMPFEHLEN SIE UNS WEITER.

www.msg.group/public