BEDAG

IT-Business Services
Technologie-Kompass 2020

Inhalt

Einleitung

Als ein führendes schweizerisches IT-Dienstleistungsunternehmen fragen wir uns regelmässig, wohin die Reise in unserem Markt geht. Dazu erstellen wir jährlich unseren Technologie-Radar, in welchem wir für unsere Softwareentwicklerinnen und -entwickler sowie für unsere Systemspezialistinnen und - spezialisten wichtige Technologien, Werkzeuge und Methoden auf ihre Einsatzfähigkeit bewerten.

Der vorliegende Technologie-Kompass ist eine zusammengefasste Version unseres internen Technologie-Radars und richtet sich an Entscheidungsträger in der öffentlichen Verwaltung. Hier gehen wir nur auf hoher Flughöhe auf einzelne Technologien und Werkzeuge ein und beschreiben IT-Trends, die wir als wichtig erachten - mit einem besonderen Fokus auf das Verwaltungsumfeld. Der Kompass erklärt aktuelle Entwicklungen und Trends in den wichtigsten Themenbereichen der IT. Er gibt einen Ausblick darauf, wie neue Applikationen aussehen werden und auf welche Aspekte bei der Beschaffung Wert gelegt werden sollte.

Öffentliche Verwaltungen müssen ständig steigenden Anforderungen gerecht werden. Einerseits müssen aufgrund neuer Gesetze und Verordnungen immer mehr und komplexere Prozesse implementiert werden. Gleichzeitig steigt die zu verarbeitende Datenmenge mit rasanter Geschwindigkeit an. Die Verwaltung steht dabei unter hohem finanziellen Druck, denn trotz den erhöhten Anforderungen sollen die Kosten reduziert werden. Auf der anderen Seite wachsen die Ansprüche der Nutzer. Sowohl die Angestellten als auch die Kunden der Verwaltung werden durch die private Benutzererfahrung von modernen Internetdiensten beeinflusst und stellen dieselben Ansprüche an die IT-Dienste der öffentlichen Hand. Ein weiteres wichtiges Stichwort ist ***Mobilität***. Mitarbeiterinnen und Mitarbeiter arbeiten nicht mehr nur zu fixen Zeiten im Büro, sondern rund um die Uhr auch unterwegs oder im Home Office. Auch die Kunden möchten ihre Geschäfte mit der Verwaltung von einem beliebigen Ort zu einer beliebigen Zeit abwickeln, am besten auf dem Smartphone.

Das Verlangen nach höherer Wirtschaftlichkeit, Digitalisierung, Mobilität und Agilität stellt Verwaltungen vor grosse Herausforderungen und erfordert eine höhere Innovationskraft der Lösungsanbieter. Kantone und Gemeinden schliessen sich zusammen, um gemeinsame Beschaffungen durchzuführen. Wenige grosse Anbieter werden zahlreichen kleinen Anbietern vorgezogen. In der Verwaltung zeichnet sich der Trend hin zu Standardlösungen und weniger Individualsoftware von Jahr zu Jahr deutlicher ab. Auch der Trend zu cloudbasierten Lösungen verstärkt sich laufend.

Gerne diskutieren wir mit Ihnen unsere Einschätzung der technologischen Herausforderungen in Ihrem Kontext.

Thomas Pischke
Technology Advisor IT-Business Services

Colin Haldemann
Leiter Engineering IT-Business Services

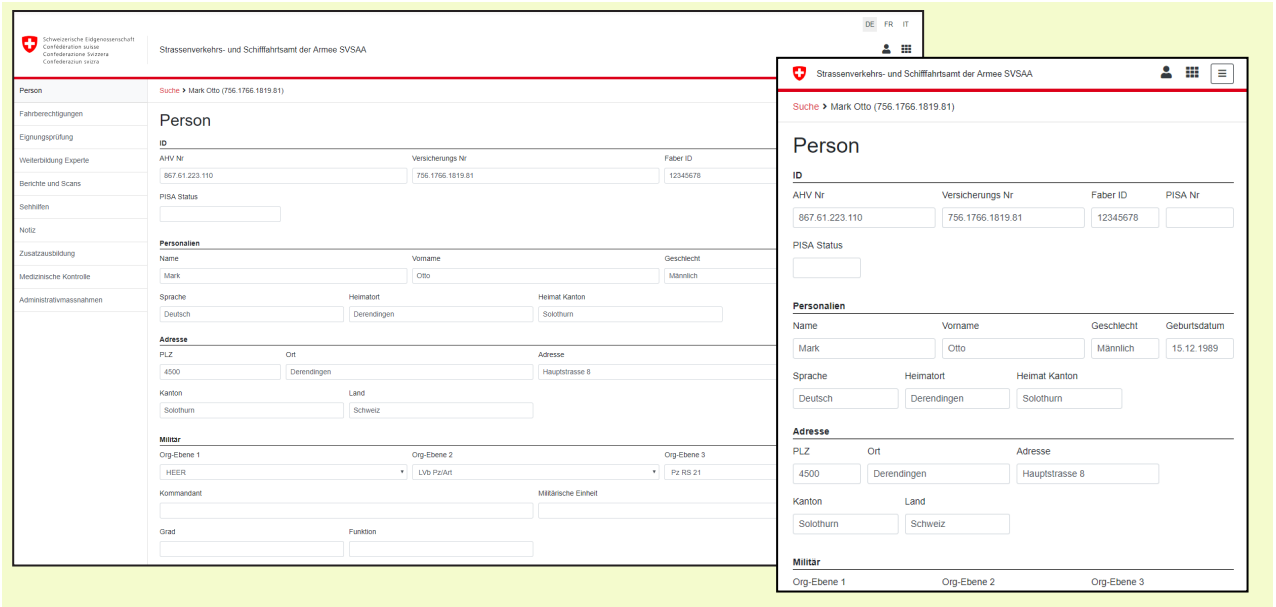
Mobilität

Wer Fachapplikationen anwendet, hat heute sehr hohe Erwartungen an die Bedienbarkeit und Funktionalität von Benutzeroberflächen. Egal ob auf dem Mobiltelefon, Tablet, Laptop oder Desktop - die Ansprüche an intuitive und effiziente Bedienbarkeit und an die zur Verfügung gestellte Funktionalität sind hoch. Reine Desktopapplikationen und Webapplikationen der ersten Generation sind heute Auslaufmodelle. Die Arbeitsprozesse von Sachbearbeitenden verändern sich stetig, hin zu mehr Mobilität, mehr Kollaboration und stärkerer Integration mit vor- und nachgelagerten Prozessen.

Dieser Wandel wird nicht nur durch die Veränderung der GUI-Technologien geprägt, sondern auch die Entstehung neuer Bedienungskonzepte wie Touchscreens, der Einsatz von Sensoren (wie z.B. GPS) bis hin zu Virtual/Augmented Reality. Die Sachbearbeiterin und der Sachbearbeiter erbringen zur Zeit den Grossteil ihrer täglichen Arbeit nach wie vor stationär an einem grossen Bildschirm mit Tastatur und Maus. Dies wird neu aber ergänzt durch einen nahtlosen Übergang auf mobile Geräte. Zu einem Termin mit den Kunden bringen die Mitarbeitenden ihr Tablet mit und können damit auf alle Informationen zugreifen und diese auch ergänzen.

Immer noch verbreitet sind Native Apps für mobile Geräte, die nur auf einem System (iOS oder Android) lauffähig sind. Zumindest im Verwaltungsumfeld werden sie aber mehr und mehr verschwinden, denn niemand will für die gleiche Funktionalität den doppelten Preis bezahlen.

Daher sollen die Fachapplikationen selber komplett mobilefähig sein. Ermöglicht wird das, indem die Webapplikationen nach dem Responsive Web Design Grundsatz entwickelt werden. So kann dieselbe Applikation auf allen Gerätetypen verwendet werden und die Benutzeroberfläche passt sich automatisch dem zur Verfügung stehenden Bildschirmplatz an. Progressive Web Apps gehen sogar noch einen Schritt weiter: Sie integrieren sich direkt in den Home Screen der Mobilgeräte und ermöglichen das Arbeiten, auch wenn die Internetverbindung einmal nicht zur Verfügung steht. Unterschiede zu einer nativen iOS oder Android-App sind für die Benutzer und Benutzerinnen kaum mehr feststellbar, die Entwicklungs- und Wartungskosten sind hingegen viel geringer.



Dateneingabeformulare sind die typische grafische Benutzeroberfläche für Fachapplikationen. Mit Responsive Web Design kann dieselbe Applikation ohne Anpassungen auf verschiedensten Bildschirmgrössen verwendet werden. Links die klassische Verwendung am Desktop PC und rechts dieselbe Maske auf einem Tablet.

Plattform

Standardisierte Container für das Deployment von Applikationen
Zentral verwaltete Applikationsserver, wie zum Beispiel Websphere oder JBoss, sind weiterhin auf dem Rückzug. Mit Docker werden Applikationen heute fertig konfiguriert und getestet, in Container verpackt und so an den Betrieb geliefert. Diese Container enthalten nicht nur die Applikation selbst, sondern auch alle von Ihr benötigten Bibliotheken, einen eigenen Webserver und sogar das Betriebssystem.

So kann der gebaute Docker-Container mit wenigen Konfigurationsanpassungen über die verschiedenen Stufen bis in den Betrieb überführt werden und es entfällt der arbeitsintensive und fehleranfällige Prozess der Installation. Probleme wie inkompatible Versionen, Konfigurationsfehler und Unterschiede zwischen den Produkten der einzelnen Hersteller, welche zu langen Verzögerungen führten, gehören damit der Vergangenheit an. Da die Updateplanung mit zentralen Applikationsservern sehr aufwändig und fehleranfällig war, wurde sie oft vernachlässigt. Dies führte dazu, dass veraltete Software auf veralteten Systemen betrieben wurde. Software in den Containern kann hingegen individuell aktualisiert werden, ohne dass Auswirkungen auf andere Applikationen zu befürchten sind. Container senken somit nicht nur die Kosten, sondern verbessern gleichzeitig auch die Sicherheit.

Nach Software as a Service sind Container das Nächstbeste zur Aufwandsminimierung wenn ein eigener Betrieb gewünscht ist. Der Softwarehersteller liefert einen fertig konfigurierten und bei ihm in genau dieser Konfiguration durchgetesteten Container an den Betreiber. Dieser muss diesen dann nur noch auf seinen Server kopieren und ausführen.

Open Source statt teure proprietäre Produkte
Der Siegeszug von Open Source setzt sich ungebremst fort. In den letzten Jahren haben grosse traditionelle Player wie Microsoft und IBM Milliardenbeträge in Open Source Firmen und Plattformen investiert und damit ein Zeichen gesetzt, dass auch die wenigen verbliebenen Kritiker verstummen lässt.

Die Entwicklung von Fachapplikationen erfolgt bereits seit längerem weitgehend mit Open Source Programmiersprachen, Tools und Frameworks. Die dabei hergestellten Fachapplikationen werden damit nicht auch automatisch zu Open Source, aber praktisch der gesamte nicht fachspezifische Code der Applikation besteht aus offenen Bibliotheken. Typischerweise beträgt der Anteil dieser Bibliotheken am Umfang der Software mehr als 80 Prozent. Die Vorteile für die Softwareentwicklung liegen auf der Hand: geringere Kosten, direkter Zugang zum Code von verwendeten Bibliotheken, eine breitere Entwicklerbasis und ein oft besserer und schnellerer Support durch die Community als durch kommerzielle Hersteller. Zudem ist in den meisten Fällen ein direkter Kontakt zu den Entwicklern des Frameworks möglich, was bei kommerziellen Frameworks nie der Fall ist.

Aus Sicht der Kunden führt diese Entwicklung zu qualitativ besseren Anwendungen und zu tieferen Kosten. Wir empfehlen Verwaltungen, bei der Beschaffung die Verwendung von Open Source als Bestandteil der Applikationen zu fordern. Wer noch einen Schritt weitergehen will, überlegt es sich, geeignete Teile seiner Applikationen unter einer Open Source Lizenz freizugeben. Der Kanton Bern hat diesen Schritt mit seiner Lösung ÖREB-Kataster bereits gemacht, ebenso wie der Bund mit seinem Corporate Design (CD Bund). So kann sich im besten Fall eine Community bilden, welche die eigene Applikation weiterentwickelt - und das kostenlos.

Continuous Delivery und agile Vorgehensmethoden
Die Automatisierung und Beschleunigung der Auslieferungsprozesse (Continuous Delivery, CD) gewinnt weiter stark an Bedeutung. Wichtige Elemente von CD sind das automatisierte Bauen der Software, wenn neuer Code geschrieben wurde (Continuous Integration, CI), das automatisierte Ausführen von Tests und schliesslich das automatisierte Ausliefern der Applikation auf gewünschte Zielsysteme.

Insbesondere in der Kombination mit agilen Vorgehensmethoden bei der Entwicklung ermöglicht CD eine massive Beschleunigung der Time-to-Market für neue Features in den Applikationen. Mit CD und Agile können folgende klassische Probleme in der Softwareentwicklung elegant gelöst werden:

- Lange Releasezyklen:
  Zwischen einem Änderungswunsch und der Auslieferung in der produktiven Software vergeht oft viel Zeit. Dieses Problem kann nicht allein mit technischen Mitteln gelöst werden, sondern muss mit einer Umstellung der gesamten Prozesse hin zu Agilität und Continuous Delivery angegangen werden.
- Unklare Anforderungen:
  Die Anforderungen an die Anwendung sind zum Zeitpunkt der Ausschreibung nicht immer klar definiert. Agile Methoden helfen dieses Problem systematisch zu lösen, indem sie laufende Veränderungen der Anforderungen nicht als Problem sondern als Selbstverständlichkeit betrachten. Durch ständige Repriorisierung der Arbeitspakete nach Business Value wird sichergestellt, dass der Kunde am Schluss qualitativ hochwertigere und genauer auf seine Bedürfnisse zugeschnittene Software erhält, als mit traditionellen Methoden. Dank der an agile Methoden angepasste Verträge (Stichwort agiler Festpreis), können diese Methoden auch bei WTO-Ausschreibungen genutzt werden. Continuous Integration unterstützt diesen Prozess, weil die Software bei kontinuierlicher Auslieferung bereits kurz nach Projektstart laufend durch den Kunden inspiziert werden kann.

Programmiersprachen
Die stetig steigenden Ansprüche der Benutzerinnen und Benutzer an die Bedienbarkeit führen dazu, dass es für Softwareentwicklende immer wichtiger wird, Programmiersprachen für das Frontend (Benutzeroberflächen) gut zu beherrschen. Wer in der Entwicklung tätig ist, muss heute also oft mehrere verschiedene Programmiersprachen anwenden können, da im Backend- und Frontendbereich meistens nicht dieselbe Programmiersprache eingesetzt wird.

Der Trend geht zur Zeit wieder verstärkt in Richtung stark typisierte Programmiersprachen, wie zum Beispiel Java, Kotlin und Typescript. Der Hype um die funktionale Programmierung ist etwas abgeflacht, weil der Paradigmenwechsel sich im Alltag manifestiert hat. Funktional geschriebene Software zeichnet sich durch geringere Fehleranfälligkeit, bessere Lesbarkeit und höhere Parallelisierbarkeit aus.

Aus Sicht der Beschaffenden sollte auf die Einschränkung des Lieferanten bezüglich Implementierungsdetails wie eingesetzte Programmiersprachen und verwendete Frameworks verzichtet werden. Die Anforderungen sollten stattdessen auf Ebene der gewünschten Zielplattform (zum Beispiel Linux, Windows, Datenbanken, Cloud) und der Schnittstellen/Interoperabilität (REST-Services, Messaging) definiert werden.

Cloudtechnologien für schnellere Releasezyklen

Mit Infrastructure as a Service (IaaS) verbinden die meisten den klassischen Cloud-Begriff. In wenigen Minuten können dort fast beliebig viele Maschinen gestartet werden. Bezahlt werden sie nur, solange sie auch verwendet werden. Der ökonomische Hintergrund dieses Geschäftsmodells sind Skaleneffekte durch die sehr hohe Anzahl gleicher Systeme und die sich ausgleichenden Bedarfsspitzen vieler Kunden.

Der Kunde erzielt durch das Verwenden einer IaaS Cloud im Wesentlichen zwei Vorteile:

- Geringere Kosten bei schwankendem Ressourcenbedarf: Wenn der Verbrauch während des Jahres stark schwankt, ist das Pay-Per-Use Modell attraktiv. Die Server kosten nur dann, wenn sie tatsächlich gebraucht werden. Es müssen zwei Voraussetzungen erfüllt sein, damit dies möglich ist: Die Applikation muss "Cloudready" gebaut sein und in der Spitze muss der Verbrauch so hoch sein, dass mehrere Server zusätzlich benötigt werden. Ist die Applikation nicht horizontal skalierbar - also auf mehrere Server verteilbar - hilft es nichts, wenn die Basisinfrastruktur dies kann. Ein erheblicher Teil der Applikationen ist heute nicht horizontal skalierbar. Zudem haben selbst die kleinsten Servereinheiten heute eine beachtliche Leistung und können mehrere hundert Benutzerinnen und Benutzer bedienen. Daher gibt es im Verwaltungsumfeld nur wenig Applikationen, bei denen die dynamische Anpassung an die Last überhaupt sinnvoll ist.
- Schnellere Installation von Applikationen, direkt durch den Lieferanten: Mithilfe einer geeigneten Private Cloud Umgebung kann der Softwarelieferant Applikationen selbstständig auf der Infrastruktur des Kunden beziehungsweise seines Betriebspartners installieren.

Cloudbegriffe

Cloudangebote lassen sich nach Art der Bereitstellung und Art der Dienstleistung einteilen.

Dienstleistung:

- Infrastructure as a Service (IaaS): Der Kunde bezieht IT-Basiskomponenten wie CPU-Leistung, Speicher und Netzwerkbandbreite. Er verwaltet alles – von der Software bis zu den Betriebssystemen – selbst.
- Plattform as a Service (PaaS): Der Kunde bezieht eine Umgebung, in die er Applikationen installieren kann. Die Plattform stellt dabei Basiskomponenten (zum Beispiel Datenbank, Applikationsserver oder Netzwerkspeicher), das Patching und Monitoring-Tools zur Verfügung.
- Software as a Service (SaaS): Der Kunde bezieht eine komplette Applikation als Dienstleistung. Diese beinhaltet als Gesamtpaket sowohl Software, Lizenzen, Updates, Betreuung als auch den Betrieb und die Überwachung.

Bereitstellung:

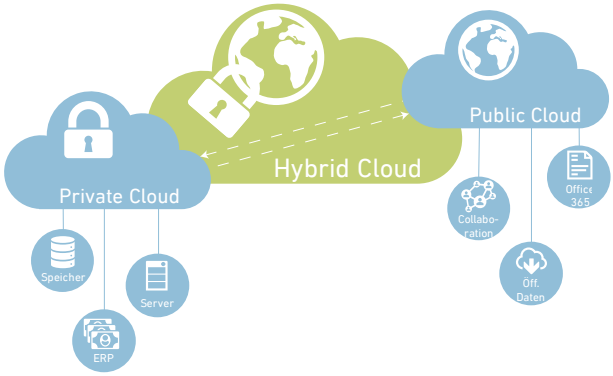
- Public Cloud: Offen, für alle im Internet verfügbar. Beispielsweise Amazon AWS oder Office 365.
- Private Cloud: Exklusiv für eine Verwaltungseinheit oder ein Unternehmen verfügbare Cloud. Wird selbst oder von einem Betriebspartner betrieben.
- Hybrid Cloud: Kombination unterschiedlicher Cloudangebote; meist public und private. So können zum Beispiel die Datenhaltung und die Funktionen getrennt bezogen werden.
- Community Cloud: Steht exklusiv einem Zusammenschluss von Organisationen zur Verfügung. Zum Beispiel eine Schweizer Verwaltungscloud.

Ein Plattform as a Service Angebot (PaaS) ermöglicht es, Applikationen effizient, schnell und fehlerfrei installieren zu können. Basisdienste, wie zum Beispiel die Datenbank, werden bereitgestellt und die Applikationen werden in einem Standardformat angeliefert. Neue Umgebungen können per Knopfdruck aufgebaut werden.

Die PaaS-Angebote sind sehr vielfältig, Docker und Kubernetes haben sich als Standard in diesem Bereich etabliert. Mit Docker können auch viele nicht für PaaS entwickelte Applikationen durch den Betreiber nachträglich "PaaS-ready" gemacht werden.

Eine PaaS-Plattform reduziert den Aufwand für den Aufbau und das Updaten von Systemen. Die Kostenersparnisse entstehen durch die Einheitlichkeit der betriebenen Applikationen. Der grössere Nutzen für das Geschäft entsteht aber häufig aus dem durch die Automatisierung ermöglichten schnelleren Releasetakt.

Im Rahmen von Software as a Service (SaaS) wird die komplette Applikation – inklusive Betrieb und allfälliger Lizenzen – als Dienstleistung vom Anbieter bereitgestellt. Bekannte Beispiele dazu sind Salesforce, Dropbox oder Gmail. Durch den Betrieb vieler Mandanten der Applikation durch einen Anbieter entstehen bedeutende Skaleneffekte. Der Anbieter ist häufig gleichzeitig auch der Softwarehersteller und kann dadurch kürzere Releasezyklen realisieren und bei Betriebs- oder Sicherheitsproblemen schnell reagieren. Aus Kundensicht muss darauf geachtet werden, dass der Betrieb professionell erfolgt. Gerade auf Basis der Public Cloud Angebote ist die Versuchung bei Softwareherstellern gross, selber ein SaaS-Angebot zu "basteln", ohne die dafür notwendigen Kompetenzen und Erfahrungen im Betrieb zu haben.
Bei den Bereitstellungsarten liegt insbesondere die Hybrid Cloud zunehmend im Trend. Die gemischte Umgebung besteht aus On-Premise Infrastruktur mit Private Cloud Diensten für datenschutzkritische Anwendungen, weniger kritische Dienste werden hingegen aus einer Public Cloud bezogen. Somit können die Vorteile beider Ansätze vereint werden. Die grossen Herausforderungen sind die Bereitstellung eines einheitlichen Identity und Access Managements (IAM), sowie die saubere Trennung der Geschäftsprozesse - nur so kann vermieden werden, dass schützenswerte Daten in der Public Cloud landen.



Mit DevOps rücken Entwicklung und Betrieb näher zusammen
Wo früher die Aufgaben und Zuständigkeiten zwischen der Softwareentwicklung und dem Betrieb klar abgetrennt waren, sind heute die Übergänge fliessend geworden. DevOps ist ein grosser Trend in der IT und wird insbesondere die grossen Firmen, wo die siloartige Trennung stark ausgeprägt ist, noch längere Zeit beschäftigen. Der Betrieb verwendet in DevOps viele der Techniken wie sie aus der Softwareentwicklung bekannt sind, wie zum Beispiel Sourcecode-Management Systeme, agile Methoden, Release-Automatisierung und Infrastructure as Code. Jedoch sind dabei nicht die Werkzeuge und Methoden von zentraler Bedeutung, sondern die enge Zusammenarbeit von Betrieb und Entwicklung in interdisziplinären Teams. DevOps ist also eher ein Kulturwandel anstatt eine neue Technologie oder Methode.

Betrieb und Softwareentwicklung arbeiten in einer DevOps Umgebung bereits beim Erstellen der Softwarearchitektur zusammen, anstatt erst ab der Inbetriebnahme. Dadurch kann die Applikation ideal auf die Betriebsarchitektur abgestimmt werden und das Know-How der Betriebsspezialistinnen und-spezialisten bereits von Beginn weg einfliessen. Im Gegenzug bauen die Betriebsverantwortlichen bereits im Laufe des Entwicklungsprojekts Know-How über die Applikation auf, was später ein effizienteres Reagieren bei Fehlerfällen im produktiven Betrieb ermöglicht.

Open Source-Technologien als Rückgrat
Im Betrieb dominiert Open Source Software längst das Feld. Open Source Lösungen sind nicht nur kostenlos verfügbar, sie bieten auch einen grösseren Funktionsumfang und sind moderner und leistungsfähiger als ihre proprietären Gegenspieler. Viele dieser Tools kommen aus dem Umfeld der grossen Internetfirmen wie Google, Twitter oder Netflix, die diese für den Gebrauch in ihren eigenen Rechenzentren entwickelt haben und sie öffentlich verfügbar machen.

Das oben bereits erwähnte Kubernetes – die Grundlage eines PaaS – wurde zum Beispiel von Google als Weiterentwicklung der internen Cloudlösung Borg als Open Source entwickelt.

Auch Red Hat (IBM) beteiligt sich sehr aktiv an der Entwicklung und benutzt Kubernetes als Basis für ihr Open Shift-Cloud-Produkt. Mittlerweile ist Kubernetes der de facto Standard für containerbasierte PaaS-Lösungen. Im Bereich der IaaS-Lösungen hat sich ebenfalls ein Standard etabliert: Praktisch alle Angebote der grossen öffentlichen Anbieter basieren auf der als Open Source verfügbaren OpenStack Plattform.

Auch für das Monitoring (Prometheus und Graphite), für das Konfigurationsmanagement (Puppet und Ansible) und für die Protokollierung (Logstash, Graylog und Elasticsearch) sind Open Source Lösungen die beliebtesten Tools.

Sicherheit ist zentral
Im Verwaltungsumfeld verarbeiten die Fachanwendungen oft Personendaten, welche gut geschützt sein müssen. Immer häufiger sollen die Anwendungen aber auch direkt über das Internet zugänglich sein, damit die Verwaltung ihre Aufgaben effizienter erfüllen kann und die Bürgerinnen und Bürger direkten Zugriff auf ihre Daten haben. Auf der Gegenseite stehen professionelle Angreifer, die nicht nur mit grossem technischem Know-how, sondern auch mit entsprechenden Finanzmitteln ausgestattet sind. Je nach Fachgebiet muss sogar damit gerechnet werden, dass ein anderer Staat gezielt Angreifer auf gewisse Daten ansetzt.

Klar, dass da auch der Schutz der Applikationen auf einem ausgezeichneten Niveau sein muss. Die Basis bildet ein guter Grundschutz im Betrieb, der auch entsprechend zertifiziert ist (ISO 27001). Heute reicht es nicht mehr aus, sich in der Sicherheitsfrage auf eine optimale Abschottung der Applikationen durch den Betreiber zu konzentrieren. Durch die Anforderung nach breiterer Verfügbarkeit der Anwendungen lassen sich diese nicht mehr abschotten. Mittels Social-Engineering-Techniken machen Angreifer auch Mitarbeiterinnen und Mitarbeiter der Verwaltungen zu unfreiwilligen Komplizen und greifen so auch eigentlich gut abgesicherte Applikationen an.

Die Softwarehersteller müssen diese Herausforderung aktiv annehmen und ihre Applikationen von sich aus auf Sicherheitslücken überprüfen und mit schneller Bereitstellung von Patches aktiv reagieren. Oft sind innert weniger Tage fixfertige Exploit Kits im Internet erhältlich, mit denen solche Lücken auch von Nicht-Experten ausgenutzt werden können. Die Reaktionszeit ist hier zentral - Es kann nicht ein Vierteljahr auf den nächsten Release gewartet werden. SaaS-Angebote haben hier klare Vorteile, da der Hersteller die entsprechenden Patches selber zentral und schnell für alle Kunden ausrollen kann.

Automatisierte Security Audits für Softwarekomponenten
Moderne Fachanwendungen werden mit zahlreichen verschiedenen Open Source Bibliotheken entwickelt. Es ist aufwändig jede eingesetzte Bibliothek regelmässig auf neu aufgetauchte Sicherheitslücken zu überprüfen, aber aus den oben genannten Gründen notwendig.

Mit automatisierten Security Audits für die eingesetzten Komponenten wird dieser Prozess zentral für alle Softwareprojekte durchgeführt. Bei grösseren Softwareherstellern mit zahlreichen Entwicklungsteams werden so starke Skaleneffekte wirksam, da die Sicherheitsüberprüfung zuvor von jedem Team separat erfolgte.

Black Duck ist eine am Markt etablierte Lösung, die für die automatischen Audits auf eine umfangreiche Datenbank von Sicherheitslücken und Lizenzinformationen zu Open Source Komponenten zugreifen kann. Black Duck führt bei jedem Build der Applikation eine Prüfung jeder verwendeten Bibliothek durch. Dabei spielt es keine Rolle, ob diese in Form von Quellcode vorliegt oder als Binärdatei. Wird eine Sicherheitslücke aufgedeckt, wird der Build verhindert, bis diese behoben wurde. Neben Sicherheitsproblemen werden auch Komponenten mit potenziell problematischen Lizenzmodellen identifiziert. Auf diese Weise kann verhindert werden, dass zum Beispiel eine Bibliothek mit einer viralen Open Source Lizenz eingesetzt wird. Die Verwendung einer solchen Bibliothek hätte zur Folge, dass die Fachanwendung ebenfalls als Open Source freigegeben werden müsste.

Daten

Flexibilität durch ereignisbasierte Systeme
Bei ereignisbasierten Systemen (Stichwort „unified log processing“) steht die Sammlung der Ereignisse im Fokus, die zum aktuellen Datenstand geführt haben. Dies steht im Gegensatz zu der bisher üblichen „statischen“ Datenhaltung in der Applikation (Attribute einer Person wie Name und Adresse werden in relationalen Tabellen abgespeichert). Die unternehmens- respektive verwaltungsweit zusammengeführte Kette dieser Ereignisse bildet nun die Kerndaten der Unternehmung. Die klassische Entitäten-/Attributesicht, wie sie in relationalen Datenbanksystemen gespeichert wird, bildet nur noch eine von mehreren möglichen Sichten auf diese Ereignisse.

Diese Architektur bietet einige Vorteile:
- ganzheitliche Sicht auf das Geschäft
- Datenstände eines beliebigen Zeitpunktes in der Vergangenheit können jederzeit rekonstruiert werden
- neue Methoden und Logiken sind auch auf die Vergangenheit anwendbar

Relationale Datenbanken als Gebrauchsgegenstand
Im Bereich der relationalen Datenbanken setzt sich der Trend, weg von den teuren proprietären Produkten wie Oracle oder Microsoft SQL Server und hin zu Open Source Datenbanken wie PostgreSQL, ungebremst fort. Diese sind den kommerziellen Produkten sowohl in Bezug auf Funktionalität wie auf Stabilität gleichwertig, verursachen aber deutlich weniger Kosten. Die relationale Datenbank ist komplett zum Gebrauchsgegenstand geworden. Die Produkte können sich nicht mehr durch Features positionieren, sondern sind komplett austauschbar.
Die Ursache dieser Entwicklung liegt vor allem in den grossen Investitionen, die Firmen wie Amazon, Alibaba und Microsoft in die Open Source Datenbanken getätigt haben. Neben PostgreSQL ist auch MySQL weit verbreitet. Seit dem Kauf von MySQL durch Oracle wendet sich die Open Source Community aber mehr und mehr von dem Produkt ab. MariaDB, ein Fork von MySQL erfreut sich hingegen immer grösserer Beliebtheit, insbesondere bei den grossen Cloud-Anbietern.

Analytics

Softwarelösungen werden smarter
Entscheidungsträger und Fachspezialisten werden zunehmend durch smarte Software direkt bei ihrer Arbeit unterstützt und entlastet. Ein smartes Softwaresystem erkennt Muster und lernt aus Daten. Je mehr Daten zur Verfügung stehen und je besser die Qualität und Struktur dieser Daten ist, desto besser kann das System daraus Vorhersagen mit hoher Treffgenauigkeit ableiten.

Ein Beispiel für smarte Software ist ein System zur automatisierten Prüfung von Steuerveranlagungen bis hin zu einer vollautomatischen Veranlagung. Weitere Einsatzbeispiele in der Verwaltung können sein:

- Erkennung von Betrug, zum Beispiel bei der Abrechnung der Mehrwertsteuer. In Belgien wird dieses System mit grossem Erfolg bereits eingesetzt.
- Predictive Policing: Anstatt nur auszuwerten, wo wie viele Einbrüche passiert sind, errechnet das System selbstständig, wo in nächster Zeit vermehrt mit Einbrüchen zu rechnen ist und hilft so bei der Einsatzplanung der Polizeipatrouillen.
- Optimierte Personaleinsatzplanung durch die genauere Vorhersage über zu erwartende Gesuche und Anfragen.

Analytics kann aber nicht einfach nur mit dem Einsatz neuer Technologien oder einem einzelnen Einführungsprojekt angewendet werden. Es erfordert einen grundlegenden Wandel der Organisation hin zu einer datengetriebenen Unternehmenskultur. Dazu gehören unter anderem die systematische Verbesserung der Datenqualität aber auch den notwendigen Zugriff auf die Daten für die Mitarbeiter zu ermöglichen.

Open Source - Auch für Analytics die erste Wahl
Um smarte Software zu erstellen ist eine Kombination verschiedener Technologien notwendig, um Daten zu sammeln und zu analysieren. Auch in diesem Sektor gibt es viele etablierte Open Source Lösungen mit breiter Nutzerbasis. Unter den Programmiersprachen für Analytics setzt sich Python zunehmend gegen die in akademischen Kreisen immer noch verbreitete Sprache R durch. Python bietet eine grosse Auswahl an Bibliotheken mit Machine Learning Algorithmen und ist die am häufigsten verwendete Sprache für Analytics. Basisbibliotheken wie NumPy, Scikit-learn oder Pandas geniessen dank der grossen Verbreitung einen ausgezeichneten Support durch die Community.

Für die Erstellung von neuronalen Netzen etabliert sich Tensorflow mehr und mehr als Standard. Anaconda, eine Plattform für Analytics etabliert sich zunehmend als die geeignete Entwicklungsplattform zum Erstellen, Testen und Trainieren von Modellen.

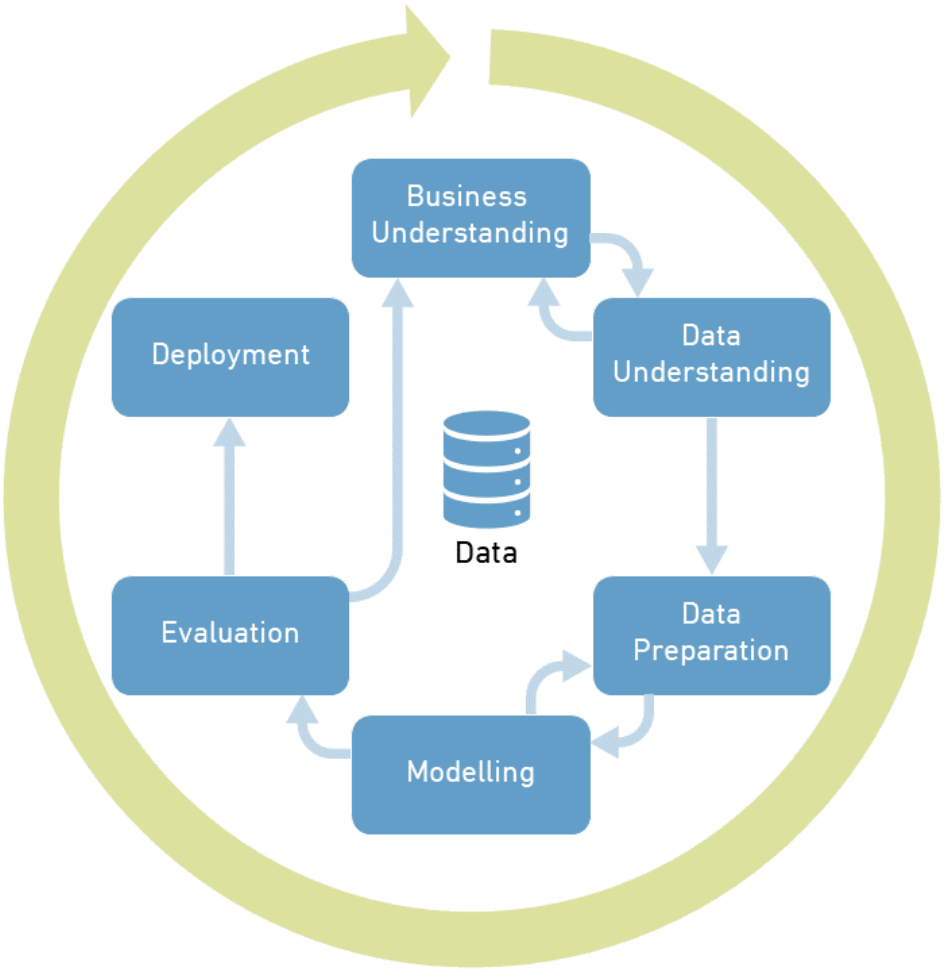
Big Data Technologien wie zum Beispiel Apache Spark sind erst für sehr grosse oder sehr schnell anfallende Datenmengen interessant. Im Verwaltungsbereich sind die Datenmengen allerdings (noch) viel zu klein, sodass der Einsatz dieser Technologien in absehbarer Zukunft nicht rentabel ist.

Als proprietäre Lösung mit Relevanz für den Bereich Analytics ist aufgrund der grossen Verbreitung der Vorgängerprodukte der Trend zu SAP HANA als performante In-Memory-Datenbank für die transaktionale Verarbeitung grosser Datenmengen ungebrochen.

Effektiver Standardprozess für Analytics-Vorhaben

Um Vorhersagemodelle für unsere smarte Software zu erstellen, verwenden wir den Cross Industry Standard Process for Data Mining (CRISP-DM). Der zyklische Prozess unterteilt die Arbeiten für Analytics-Vorhaben in sechs Phasen, die grundsätzlich sequentiell abgearbeitet werden.

Das Softwaresystem wird laufend verbessert, indem man nach der Inbetriebnahme der Lösung mit dem CRISP-Kreislauf wieder von vorne beginnt. Dadurch kann in nachfolgenden Iterationen die Genauigkeit mithilfe der zuvor gewonnenen Erfahrungen weiter gesteigert werden.



Integration

Microservices – agilere IT
Anstatt als grosse, voll integrierte Applikationsmonolithen werden Lösungen heute vermehrt aus kleinen, in sich abgeschlossenen Diensten aufgebaut. Jeder Dienst ist dabei für genau eine klar abgegrenzte Geschäftsfunktion zuständig und hat seinen eigenen Lebenszyklus.

Aus wirtschaftlicher Sicht vermindern Microservices negative Skaleneffekte in der Softwareentwicklung. Es gilt der Grundsatz: Je grösser die entwickelte Applikation, desto weniger effizient erfolgt die Entwicklung aufgrund der zunehmend notwendigen Koordination. Dies führt dazu, dass jede zusätzliche Entwicklerin oder jeder zusätzliche Entwickler immer weniger zusätzliche Ergebnisse produziert. Die optimale Produktivität wird erreicht, wenn eine Applikation von maximal sieben Personen erstellt werden kann.

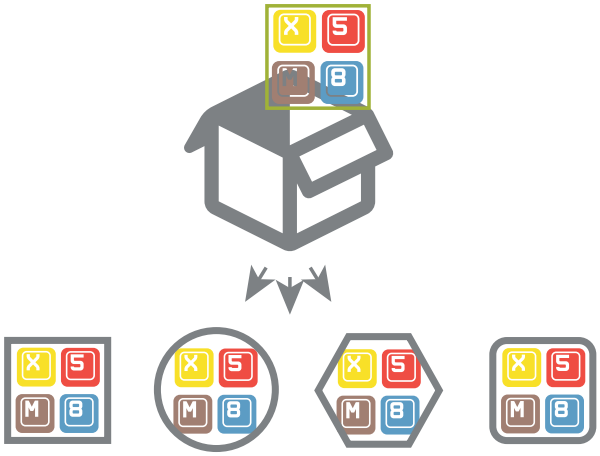
Mit dem Microservice-Ansatz werden Applikationen in voneinander weitgehend unabhängige Dienste aufgeteilt, für die jeweils ein kleines Team zuständig ist.

Die Microservice-Architektur erweitert die mittlerweile etablierte serviceorientierte Architektur (SOA) in folgenden Punkten:

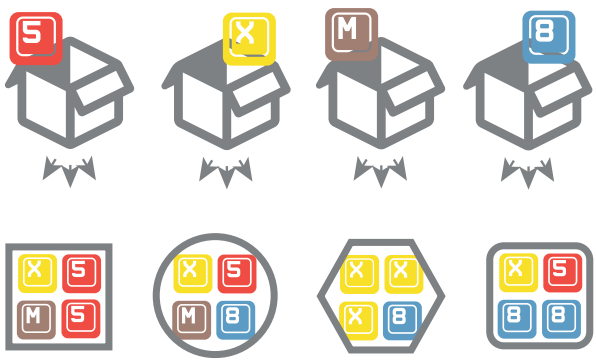
- Schlaue Endpunkte statt Enterprise Service Bus (ESB): In einer klassischen SOA wird oft versucht, die Komplexität in einem zentralen ESB zu verstecken. Auf Microservice basierte Architekturen verzichten bewusst auf ESB und setzen auf Informationsaustausch auf der Basis einfacher Protokolle (meist REST).
- Dezentrale Verwaltung: Jeder Microservice wird von einem eigenständigen Team mit einem eigenen Releaseprozess gepflegt. Damit wird der Koordinationsaufwand stark verringert. Auch die Releasezyklen können so verkürzt werden, bis hin zu wenigen Tagen.
- Dezentrale Daten: Die Daten werden pro Microservice isoliert gehalten. Es ist also kein direkter Datenzugriff über die Servicegrenzen möglich. Jeder Dienst hat seine eigene Datenbank.
- Kleinere Granularität: Microservices haben typischerweise einen kleineren (Funktions-)Umfang als ein Service im Sinne von SOA.

Haupttreiber für die Microservice-Architektur ist das Bedürfnis, von den trägen Releaseprozessen wegzukommen. Weder Unternehmen noch Verwaltungen können es sich heute leisten, länger als ein paar Wochen auf wichtige neue Geschäftsfunktionen zu warten. Aus Sicht einer Verwaltung sollte darauf geachtet werden, dass nicht grosse, monolithische Systeme erstellt beziehungsweise beschafft werden, sondern auf eine modulare Architektur gesetzt wird.

Monolithische Anwendung



Microservices-Architektur



Öffentliche Schnittstellen machen eGovernment effizienter und günstiger
Die meisten existierenden eGovernment-Lösungen sind entweder für den einzelnen Bürger oder aber für grössere Unternehmen ausgelegt. Angebote für den Bürger haben eine einfach zu bedienende Benutzeroberfläche, sind aber für die Erfassung grösserer Datenmengen nicht geeignet. Ein Beispiel hierfür sind die Weblösungen der Strassenverkehrsämter: Für grosse Transportunternehmen sind diese unpraktisch, da sie sich nicht in ihre Systeme integrieren lassen. Dem gegenüber stehen Lösungen, die explizit für Unternehmen konzipiert wurden. Diese lassen sich sehr gut integrieren und bieten zusätzliche Funktionen, allerdings bringen sie komplizierte Schnittstellen und komplexe Einrichtungsprozessen mit sich.

Als Lösungskonzept zur Überbrückung dieser Lücke eignen sich öffentliche API (Application Programming Interface):

Die Verwaltungssysteme veröffentlichen einen Teil ihrer Geschäftsfunktionen als vom Internet her zugängliche technische Dienste (Webservices) und zwar unabhängig von konkreten Verwendungsszenarien. Der Zugriff wird selbstverständlich geschützt, sodass jeder Bürger und jedes Unternehmen nur auf seine Daten zugreifen kann. Optimalerweise werden genau dieselben Dienste auch intern – also vom Amt selbst oder von anderen Ämtern – verwendet. Technologisch handelt es sich typischerweise um REST-Services.

Das Konzept der öffentlichen Schnittstellen ermöglicht unzählige neue Anwendungen die es Bürgern und Unternehmen erlaubt dynamischer und schneller mit der Verwaltung zu interagieren, wie die folgenden Beispiele zeigen:

- Eine Schnittstelle für die Erfassung von Steuerbelegen kann sowohl von einer ERP-Software eines Unternehmens, wie von einer Handy-App für Einzelunternehmen eingebunden werden.
- Ein Hersteller von Software für Autogaragen erweitert seine Software so, dass das Anmelden von Fahrzeugen zur Inspektion direkt aus der Applikation möglich wird. Auch hier kann der Bürger mit einer Handy-App eines anderen Herstellers den Prüfungstermin für sein Auto über dieselbe Schnittstelle festlegen.
- Fachapplikationen der Ämter können sich die aktuellste Adresse der von ihnen geführten natürlichen und juristischen Personen über eine zentrale Schnittstelle der kantonalen Personenregister liefern lassen. Dieselbe Schnittstelle könnte auch ausgewählten privaten Organisationen zur Verfügung gestellt werden.

All diese Angebote verwenden also in verschiedenen Szenarien die identischen Schnittstellen, welche das Amt mit einer einmaligen Softwarebeschaffung zur Verfügung stellt.

sedex mit eCH-Standards
Für den privaten Meldungsaustausch zwischen Behörden wird sich sedex noch weiter etablieren. sedex bietet eine sichere und zuverlässige Plattform zum Austausch von Meldungen zwischen Organisationen. Trotz der technisch einfach ausgelegten Schnittstelle auf Dateisystemebene und der damit verbundenen etwas schwerfälligen Handhabung, sowie des begrenzten Meldungsdurchsatzes ist es der einfachste und zuverlässigste Übertragungsweg. Als Format für die ausgetauschten Meldungen werden in fast allen Fällen Standards des Vereins eCH verwendet. sedex Pathfinders erweitert sedex zusätzlich um eine Möglichkeit zur synchronen Kommunikation mittels einem Webservice.

Dokumente

Dokumente – verborgene Daten
Immer noch werden viele geschäftsrelevante Daten in Dokumenten zum Beispiel im Word oder Excel Format abgelegt. Diese Daten sind nur schwach oder gar nicht strukturiert und eignen sich deshalb schlecht für automatisch erstellte Auswertungen und automatisierte Weiterverarbeitung. Diese automatisierbaren Prozesse sind aber die notwendige Basis für die Transformation hin zu einer datengetriebenen Organisation (siehe Kapitel Analytics).

Will man die digitale Transformation vorantreiben, so sollten Daten also wenn immer möglich in einer möglichst stark strukturierten Form erfasst werden um sie damit maschinenlesbar, und -auswertbar zu machen. Sinnvolle Ansätze dazu sind die Integration in eine Fachlösung oder die Nutzung spezialisierter Systeme, die den Benutzer bei der Erfassung der Daten unterstützen. Als Endprodukt kann dabei immer noch ein Blatt Papier entstehen. Allerdings ist dieses dann aus den Daten generiert und nicht der primäre Datenträger. Zusätzlich ist es so auch für den Empfänger möglich, die Daten elektronisch zu verarbeiten. Ein Unternehmer könnte zum Beispiel seine Veranlagungsverfügung direkt wieder in seine Steuersoftware einlesen.

Strukturierte Daten generieren Business Value
Als einfach realisierbare Verbesserung können die internen Abläufe zwischen mehreren Stellen statt via E-Mail versandte Word-Dokumente in einem Vorgangsverfolgungssystem wie Atlassian JIRA abgebildet werden. Dies kann zum Beispiel für Personaleintritte oder das Beantragen von Berechtigungen, aber auch für viele weitere Prozesse angewendet werden. Die Daten werden so strukturiert erfasst und können trotzdem noch mit Bemerkungen ergänzt werden. Auswertungen über die Bearbeitungszeit, Engpässe, Inhalt und Art der Anfragen können einfach erstellt werden. Zudem können die strukturiert vorliegenden Daten nun auch als Rohdaten für Data Analytics dienen. Es können Vorhersagemodelle erstellt werden, mit welchen einfache Arbeitsabläufe automatisiert oder mit Entscheidungshilfen ergänzt werden können.

Formulare – immer noch wie auf dem Papier?
Die Möglichkeiten elektronischer Formulare werden immer noch ungenügend genutzt:

- Keine Anbindung an die Systeme: Nach der erfolgten Erfassung entsteht ein Medienbruch. Die Daten werden per E-Mail übermittelt oder sogar ausgedruckt und nicht digital in das zuständige System (Ticketing, Fallmanagement oder sonstige Fachapplikationen) überführt.
- Fehlende Benutzerführung: Elektronische Formulare eignen sich optimal, um den Benutzer bei der Erfassung der Daten anzuleiten und mit kontextabhängigen Feldern und Zusatzinformationen zu führen. Allerdings sind die meisten elektronischen Formulare heutzutage immer noch eine Kopie der statischen Papierformulare.

Was ausserdem oft vergessen geht: Vielfach sind die Daten beim Anfrager, also bei der Bürgerin oder dem Bürger oder beim Unternehmen, bereits in einem System vorhanden. Dadurch führt alleine das Ausfüllen des Formulars durch den Anfrager zu einem ersten Medienbruch und zu potenziellen Fehlern. Zu jedem Formular sollte immer auch eine entsprechende öffentlich verfügbare Schnittstelle (siehe Kapitel Integration) existieren, damit die Daten auch maschinell eingeliefert werden können.

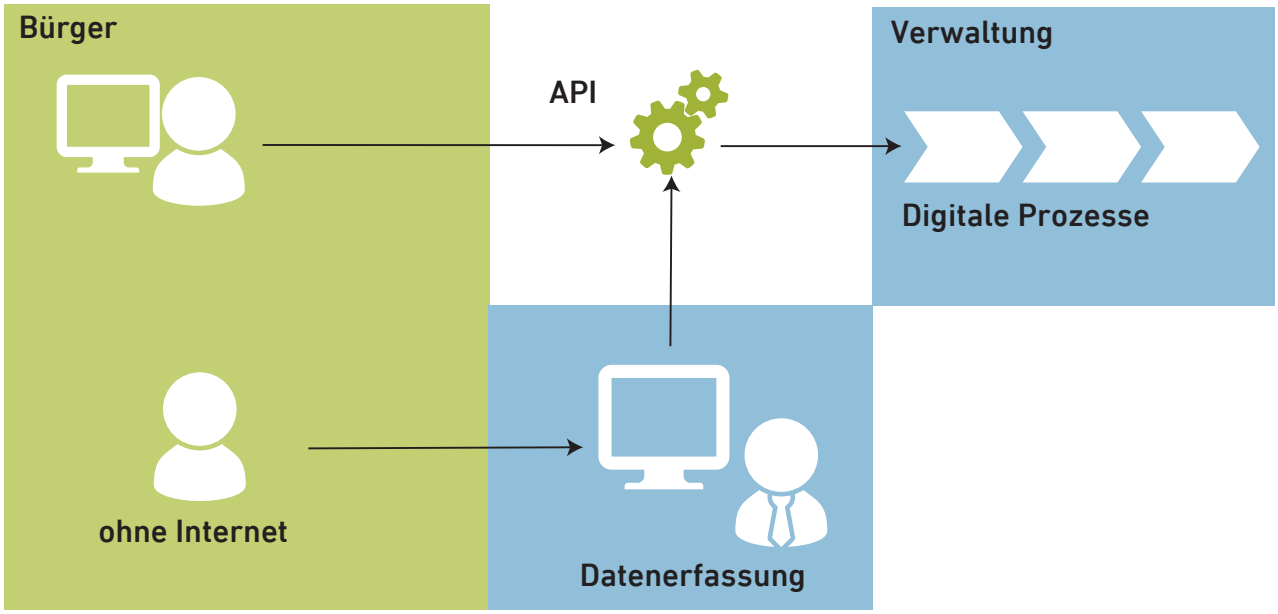
Digitale Identität und Signaturen - Es geht voran
Elektronische Signaturen und Identitäten sind die letzte Hürde für die Erstellung rein digitaler Prozessabläufe mit rechtlich verbindlichen Unterschriften. Trotz grosser Bemühungen von Akteuren wie dem SwissID Konsortium und dem Gesetzgeber ist das Interesse in der Bevölkerung noch kaum Vorhanden - Bisher fehlt die Killerapplikation.

Für Online-Dienste der öffentlichen Verwaltung, die allen Bürgerinnen und Bürgern zugänglich sind, werden sich vielseitig nutzbare

Lösungen wie die SwissID mehr und mehr durchsetzen. Es ist für Behörden nicht mehr sinnvoll eigene (klassische) Logins anzubieten, da diese höhere Administrationsaufwände mit sich bringen (Stichwort "verlorene Passwörter"). Dies insbesondere, wenn noch eine Beglaubigung der Personenidentifikation hinzukommt, zum Beispiel für das Online-Einreichen der Steuererklärung.

Der Zusatznutzen einer digitalen Signatur gegenüber der digitalen Identität liegt darin, zu einem späteren Zeitpunkt dem Absender zweifelsfrei belegen zu können, dass er diese Daten genauso übermittelt hatte und das Amt diese nicht verändert hat. Dies ist häufig aber gar nicht erforderlich.

Digital Divide – nicht alle sind im Internet
Gerade für Verwaltungen ist der Digital Divide eine grosse Herausforderung. Im Unterschied zu Unternehmen können sie nicht einfach aus Effizienzgründen jene Kundinnen und Kunden ohne Zugang zum Internet von ihren Dienstleistungen ausschliessen. Sie haben die Pflicht, sämtliche Bürgerinnen und Bürger zu bedienen. Das bedeutet, dass Papierprozesse weiterhin erhalten bleiben müssen. Die Effizienz soll aber trotzdem gesteigert werden. Ein erfolgsversprechender Ansatz ist, die kompletten Prozesse zu digitalisieren, dabei aber darauf zu achten, dass saubere, maschinennutzbare Schnittstellen definiert werden (siehe Kapitel Integration). Auf Basis dieser Schnittstellen kann an einer zentralen Stelle ein gezielter Übergang von/zu Papier erfolgen. Dieser Ansatz muss weiter gehen, als einfach nur die Papiere zu scannen, da dies alleine die Daten noch nicht verwertbar macht. Die Daten müssen von einem Datenerfassungsteam oder einer smarten analytics-gestützten Software zu einem Aufruf der Standardschnittstelle aufbereitet werden.



Über die Bedag Informatik AG

Die Bedag ist mit einem Umsatz von über 80 Mio. Franken ein führendes schweizerisches IT-Dienstleistungsunternehmen. Mit ihren rund 370 Mitarbeiterinnen und Mitarbeitern – wovon 32 Lernende – verfügt sie über ein breites und fundiertes Informatik-Know-how. Ihr Kerngeschäft ist die Entwicklung, die Wartung und der Betrieb von geschäftskritischen Informatiklösungen. Damit ermöglicht sie ihren Kunden einen wirtschaftlichen und sorgenfreien Informatikeinsatz. Mit einem Netz von hochsicheren Rechenzentren sowie Standorten in Bern, Aarau, Delémont und Wettingen ist sie regional stark präsent. Ihre Kunden sind hauptsächlich öffentliche Verwaltungen und Betriebe, sowie Unternehmen im Gesundheits- und Versicherungswesen. Die Bedag wurde 1990 gegründet und befindet sich im Eigentum des Kantons Bern.
www.bedag.ch

Bedag Informatik AG
Engehaldenstrasse 12
Postfach
3001 Bern

Tel. 031 633 21 21
info@bedag.ch
www.bedag.ch