KI-Projekte in Behörden beginnen

– Whitepaper –

Werkstatt „Digitale Projekte“

1. Ziel und Umfang

Dieses Whitepaper ist für interessierte Pragmatiker geschrieben, die als IT-Verantwortliche oder Projektmanager der öffentlichen Verwaltung arbeiten und noch keine Erfahrungen mit Projekten in künstlicher Intelligenz (KI) gesammelt haben. Es soll auf allgemeinem Niveau beschreiben, welche Entscheidungen getroffen und welche Voraussetzungen vorhanden sein müssen, um in das Feld KI einzusteigen und ein erstes Projekt zu beginnen. Der Text gibt also Antworten auf diese Fragen:

- Wofür und wann ist der Einsatz von KI sinnvoll?
- Was sind Besonderheiten von KI?
- Wie identifiziere ich ein geeignetes Projekt?
- Welche Voraussetzungen muss ich für ein erstes Projekt erfüllen?
- Welche Schritte führen zum Projekterfolg?
- Was sind Risiken und Empfehlungen auf dem Weg, unter Berücksichtigung einer typischen Behördenstruktur?

2. KI und *machine learning*

In den letzten Jahren hat sich die künstliche Intelligenz, KI, zum innovativsten Gebiet der IT entwickelt. Ursache dafür sind ganz eindeutig die massiven Fortschritte auf dem Gebiet des *machine learning* (ML). In fertigen Algorithmen, ausgereiften Entwicklungsumgebungen und mit gewachsener Hardware-Performance ist die die Technik nun leicht zugänglich und anwendbar. Es ist absehbar, dass keine andere aktuelle Entwicklung die IT und ihre Anwendung so vielfältig beeinflussen wird. Ursache dafür sind die revolutionären Fähigkeiten von trainierten ML-Systemen in Mustererkennung und Analyse. Sie werden vielfältig in Forschung und kommerziellen Produkten angewendet bei der Erkennung von Bildinhalten oder Sprache, von Strukturen und Ähnlichkeiten bei Bildern, Musik, Begriffen oder Texten, letzteres vor allem für Suche oder Übersetzung. Neuronale Netze können Bilder, Sprache und Videos verändern und konstruieren und mittlerweile auch auf abstrakten Wegen Ziele erreichen, was sie mit strategischen Fähigkeiten beweisen. In vielen dieser Anwendungen sind KIs nicht nur schneller als klassische Software, sie sind diesen vor allem in den Ergebnissen deutlich überlegen.

Natürlich sind Risiken für diese neue Technologie zu betrachten und Regularien dafür zu einwickeln. Gerade in Deutschland erfolgt darüber eine intensive Diskussion mit einer Reihe von Studien. Dabei wird aber manchmal vernachlässig, dass es auch wichtig ist, auf den Feldern auch konkrete Erfahrungen mit der Entwicklung und der Nutzung von KI zu sammeln. Dabei soll dieses Whitepaper helfen.

Die oben beschriebenen Leistungen von KI erfüllen viele Anforderungen, die auch bei Behörden relevant sind. Trotzdem wird im öffentlichen Sektor, nach Stand des Jahres 2020, selbst entwickelte KI nur in einer überschaubaren Zahl von Fällen genutzt. Etwas verbreiteter sind Automatisierungswerkzeuge, Entscheidungssysteme und Kommunikationshilfen, vor allem Chatbots, oft von kommerziellen Anbietern.

Erfahrungen mit echtem ML auf der Basis von eigenem Code und trainierten Systemen gibt es vor allem in Behörden mit einem ausreichend großen Bereich für Softwareentwicklung. Eines der Ziele von NExT ist es, die Grenzen der „Silos“, wie Behörden sie gerne bilden, aufzubrechen. Entsprechend werden innerhalb der Mitglieder von NExT Erfahrungen mit KI und ML übergreifend ausgetauscht, um so voneinander zu lernen. Einige für Behörden geeignete Anwendungsfelder, dabei diskutiert wurden:

- Anomalieerkennung zur Betrugsbekämpfung;

- E-Mailfilterung und automatische Bewertung;
- die Analyse digitaler Eingaben und Formulare, auch um automatische Abläufe vorzubereiten und zu verbessern;
- Analyse von großen Datenmengen, etwa Signale aus IT-Systemen, um eine höhere Verfügbarkeit und Sicherheit zu erzielen.

Mit diesem Whitepaper wollen wir daraus allgemeine *best practices* für die Entwicklung mit KI in Behörden ableiten, um den Einstieg in das Feld zu erleichtern und damit die großen Vorteile im öffentlichen Bereich leichter angewandt werden können. Entsprechend fokussieren sich die folgenden Abschnitte auf eine **praktische Umsetzung in einer Behörde**, also darum, wirtschaftliche und realisierbare Projekte vorzubereiten und durchzuführen.

Der Begriff KI wird inflationär gebraucht und kann genutzt werden, um das sich entwickelnde Feld zu bezeichnen, natürlich ohne dass damit eine echte Intelligenz bezeichnet würde. Wir konzentrieren uns im Folgenden spezifisch auf **Projekte mit *machine learning***. Dies bezeichnet Software-Systeme, in denen mit umfangreichen Eingabedaten neuronale Netze trainiert werden, um selbstständig Abhängigkeiten zu erkennen und aus diesen dann Wahrscheinlichkeiten für Ergebnisse zu errechnen. Alle genannten Fortschritte der letzten Jahre wurden mit *machine learning* erzielt, und die Methode ist erstaunlich rasch zu implementieren. Erfahrungen mit Entscheidungssystemen der maschinellen Prozess-Automatisierung werden nur am Rande betrachtet. Diese sind seit längerem am Markt verfügbar und haben ein etwas anderes Einsatzfeld.

Wir sehen KI mit ML dabei nicht als grundsätzlich neues Verfahren, sondern verstehen es als eine **moderne Erweiterung der bisherigen Software-Entwicklung**, bei der man auf bestehender Projekterfahrung aufbauen kann.

3. Auswahlkriterien für KI-Projekte in Behörden

In einer Behörde ist die Projektleitung oft gefordert, die zentralen Faktoren eines Projektes vorab abzuschätzen, also vor allem den Zeitaufwand und die Kosten genau zu benennen. Dies ist bei einem agilen Softwareprojekt ohnehin nur noch in bestimmten Grenzen möglich. Beim ersten KI-Projekt kann man sich zudem nicht auf Erfahrungswerte berufen. Um das Gesamtrisiko zu verringern, empfehlen wir, den Umfang eines ersten KI-Projektes **so klein wie möglich** zu wählen und ein **einfach erreichbares Ziel** zu suchen. Ein Beispiel dafür kann sein: „Wurden in einem einfachen Formular in allen üblichen Feldern Einträge vorgenommen?“ im Gegensatz etwa zum ambitionierten: „Wurden in einem Formular alle Felder *sinnvoll* ausgefüllt?“. Es ist realistischer, bei Erfolg das Projekt in einem zweiten Schritt zu erweitern, als sich ein nicht erreichbares Ziel zu setzen. Das erste Projekt sollte also vor allem geeignet sein, Software-Entwicklung mit ML kennenzulernen.

Wichtigstes Kriterium für ein *machine-learning*-Projekt ist eine ausreichende Anzahl von **verfügbaren, klassifizierten Daten**. Für die allgemeine Orientierung: ein ML-Netzwerk benötigt für das Training mit überwachtem Lernen eine Größenordnung von über tausend, besser **mehreren tausend Datensätzen**. Viel hängt natürlich von Art und Umfang der Daten ab, sowie davon, dass die Projektteilnehmer die Inhalte kennen und interpretieren können. Eine hohe Qualität der Daten kann die erforderlichen Datenmengen verringern. Dies kann auch durch Filterung und Vorbearbeitung erzielt werden, was umgekehrt aber die Projektzeit in dieser Phase verlängert. Ebenso können weniger Trainingsdaten ausreichen, wenn man niedrige Ansprüche an die Qualität der Vorhersage stellt, etwa eine Genauigkeit von 85% akzeptiert oder ein eigentlich einfaches Ergebnis anstrebt, etwa „hell“ oder „dunkel“.

Für das erste Behördenprojekt sollten nicht schützenswerte Daten ausreichend verfügbar sein

Trainingsdaten sollten unabhängig vom Typ möglichst **gleichförmig** vorliegen, so zum Beispiel als Einträge in einer relationalen Datenbank, großer Satz gleichartig gescannter A4-Seiten, Bilder gleicher Größe oder gleichartig strukturierte Textdateien wie Emails. Alle Daten müssen vorab gesichtet und dem gewünschten Ergebnis, das die KI produzieren soll, entsprechend bewertet sein. Daten könnten z. B. klassifiziert werden in „komplett“ oder „unvollständig“, „Katze” oder „Hund”, „sehr wichtig“ bis „völlig unwichtig“. Die **Klassifizierung** („labeling“) der Daten durch Menschen kann in günstigen Fällen bereits in Metadaten vorhanden sein, andernfalls muss diese eine Phase des Projektes werden.

Die Auswahl von Datensätzen zum Training ist wichtiger und hat weitergehende Auswirkungen, als es am Anfang erscheinen mag. Tendenzen und Gewichtungen in der Auswahl der Quelldaten oder Bewertung der Zieldaten wird eine KI lernen und übernehmen, ähnlich wie Schüler Ansichten von Lehrerin und Lehrer übernehmen. Die Besonderheiten und Risiken der Datenauswahl bei einem KI-Projekt sollten allen Teilnehmenden im Projekt bewusst sein, also gerade auch der Fachseite außerhalb der IT-Entwicklung. Es ist empfehlenswert, sich vorab auf diesem Gebiet fortzubilden, entsprechende Grundlagen werden in Studien und Kursen auch frei online vermittelt. Mehr Details zu diesem Thema und die Betrachtung des daraus entstehenden Regelungsbedarfes würden aber den Rahmen dieses Whitepapers sprengen. NExT plant daher, die Themen Datenauswahl, Datenbearbeitung, Datenschutz und synthetische Daten bei Behörden-KI in einem kommenden weiteren Whitepaper zu behandeln, zusammen mit spezifischen Aspekten der IT-Sicherheit.

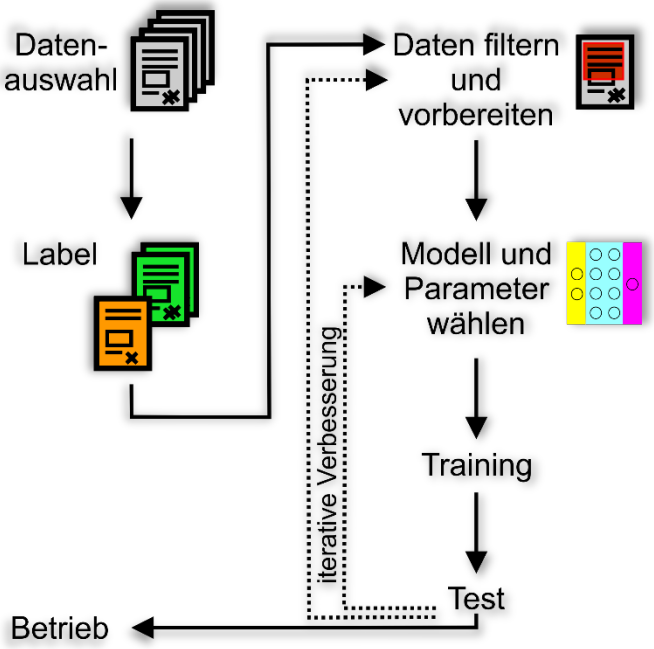
In jedem Fall ist zu empfehlen, keine personenbezogenen Daten für das erste Projekt zu nutzen oder diese vorab auszufiltern. So könnten etwa Namensfelder bei dem als Beispiel angeführten Formularprojekt ignoriert oder mit künstlichen („synthetischen“) Testdaten gefüllt werden, oder man beschränkt sich auf die Grauwerte der unterschiedlichen Felder, ohne dass der Inhalt des Feldes ausgelesen wird. Datenschutz-Aspekte und den Umgang damit sollte die Projektleitung mit dem Projektcontrolling und den Gremien der eigenen Organisation klären. Datenschutzmaßnahmen können auch die Qualität der Ergebnisse verringern, daher ist es besser, nicht schützenswerte Daten auszuwählen.

Für die Entwicklung von Behörden-Software müssen noch weitere Besonderheiten des ML erläutert werden. Zwar werden in vielen IT-Projekten einfache Entscheidungsabläufe in Software übertragen und automatisiert, aber ein erstes, so bezeichnetes „KI“-Projekt wird möglicherweise besonders intensiv hinterfragt. Der Ablauf einer KI ist aber nicht mehr, wie in

einer klassischen Programmiersprache, über den Programmtext nachvollziehbar. Natürlich ist auch eine KI Programmcode und dieser ist reproduzierbar. Eine KI wird also immer genau dieselben Ergebnisse produzieren, sofern die Eingangsdaten identisch sind und Trainingsdaten und Trainingsparameter, etwa der Zahl der Ebenen des neuronalen Netzes mit einer nicht zufälligen Anfangsgewichtung der Knoten, gleich bleiben.

Es ist aber äußerst aufwändig nachzuvollziehen, welche Abhängigkeit ein neuronales Netz zwischen Eingangs- und Ausgangsdaten im Detail herstellt. An Stelle von den Programmstatements in klassischer Software, etwa einer „Wenn-dann"-Bedingung, treten sehr umfangreiche Gleichungssysteme. Diese beschreiben zum Beispiel die Wahrscheinlichkeit, mit der zwei spitze Dreiecke über einem Kreis den Kopf einer Katze bedeuten. Es macht gerade die Stärke von KI aus, dass ein Software-Entwickler diese Abhängigkeiten nicht mehr selbst in Algorithmen fassen muss, sondern dass diese Leistung automatisiert im Training erbracht wird. Das Software wird dadurch viel schneller erstellt und liefert in der Regel genauere Ergebnisse, als wenn Menschen dies programmieren würden. Dieser Ablauf stellt eine neue Form des „codings" dar, der mit einem Verlust von Detailkenntnissen bezahlt wird.

Aus dieser Besonderheit des ML folgt, dass man sich in einem Projekt nicht die Mühe macht, den Programmcode einer ML-Software nachzuvollziehen oder gar Teile davon zu korrigieren, wenn sie unverständliche Ergebnisse liefert. Stattdessen wird man sie mit veränderten Eingangsdaten oder verbesserten Rahmenparametern neu trainieren. Es ist nur für Experten möglich, abzuschätzen, warum eine KI bei einem einzelnen Datensatz zu einem bestimmten Ergebnis kommt. Hier bieten algorithmische Entscheidungssysteme als KI-Alternative einen Vorteil, da bei diesen die Abläufe klarer und nachvollziehbarer beschrieben werden können.



Ein ML-Projekt durchläuft andere Phasen als die bislang etablierte Software-Entwicklung

Nicht unerwähnt bleiben sollte der Unterschied im Zeitaufwand. In einem erfahrenen Team ist eine KI in einigen Wochen trainiert. Ein Projekt mit einem Ziel, bei dem ML seine Stärken ausspielen kann, wird unter den richtigen Voraussetzungen bis zu einem Faktor 10 schneller abgeschlossen sein, als dies ohne ML-Einsatz möglich wäre.

Diese Erfahrungen zu den Unterschieden klassischer Programmierung zu sammeln, sollte ein wichtiges Ziel eines ersten Projektes sein. Diese Besonderheit des ML ist auch zu berücksichtigen, wenn man auswählt, welche Daten die Software bewertet und welche Entscheidungen sie nachvollziehen soll. Es ist davon abzuraten, sensible Verwaltungsprozesse durch eine KI bewerten zu lassen. Zu vermeiden sind Abläufe, die gewichtige Eingriffe oder strafrechtliche Folgen bedeuten, selbst wenn die KI am Ende nur eine Empfehlung erstellt. Sinnvoller ist die Klassifizierung von Daten aus unbedenklichen Standard-Prozessen. Als Beispiel kann wieder einmal die beschriebene Prüfung dienen, ob ein Formular vollständig ausgefüllt

wurde oder die Wahrscheinlichkeit, dass eine eingegangene E-Mail als wichtig gekennzeichnet wird.

In jedem Fall sollte eine KI die Entscheidung eines Menschen lediglich unterstützen. Ergänzend sollte organisatorisch immer ein Kontrollprozess vorgesehen werden, durch den die Empfehlung des automatischen Systems in Stichproben oder nach Widerspruch geprüft wird, und zwar durch einen Menschen mit Fachkenntnis, der die Entscheidung korrigieren und revidiert kann. Beim Betrieb der Software sollte diese Kontrolle im Verwaltungsprozess etabliert sein.

4. Projektstruktur

Das KI-Projekt sollte aus einer Projektgruppe entstehen, bei der alle Mitglieder mit IT-Projekten Erfahrung haben, bereit sind und ausreichende Zeit zur Verfügung haben, um sich mit den Besonderheiten und Risiken von KI vertraut zu machen. Diese sind in diesem Text nur angerissen, aber es sind umfangreiche Kurse und Lerninhalte verfügbar. Eine optimale **Teamstruktur** beinhaltet:

a. einen Projektmanager oder eine Projektmanagerin, vertraut mit agilem Vorgehen und versehen mit zusätzlichen Ressourcen für den Fall von Projektrückschlägen;
b. einen oder mehrere Software-Entwickler, die mit ML oder dem ansonsten gewählten Verfahren mindestens theoretische Kenntnisse haben;
c. Spezialisten, die die verwendeten Daten kennen, digital analysieren, filtern und aufbereiten können („data scientists“, siehe auch 5e im nächsten Abschnitt);
d. Fachpersonal, das die Eigenschaften, die Entstehung und den Weg der Daten kennt, Anforderungen an das Produkt stellen und das Ergebnis bewerten kann;
e. eine Leitungsebene, die technischen Neuerungen aufgeschlossen gegenübersteht und die Notwendigkeit versteht, hier Erfahrungen zu sammeln;
f. Sicherheits- und Schutzbeauftragte, die bereit sind, die regulatorischen Abläufe bei Entwicklung und Verarbeitung zu prüfen und darüber zu entscheiden, auch wenn diese von klassischen IT-Projekten abweichen;
g. weitere Beratung und Expertise bei Bedarf für besondere Fragen zu Daten, KI-Technik oder Projektmanagement.

Technische Projektressourcen umfassen:

h. einen Pool von für das Projekt freigegebenen, klassifizierten Datensätzen in der Größenordnung ‚tausende‘;
i. eine lokale Entwicklungsumgebung, möglichst mit etabliertem Verfahren für Release-Management;
j. je nach Datenvolumen eine Hardware-Kapazität von einem, eventuell mehreren Servern für das Training;
k. eine Produktivumgebung, mit der die Produktivdaten an die trainierte Software weitergegeben werden können und die daraus das Ergebnis ermittelt und darstellt, z. B. einen Workflow-Engine oder ein Webserver mit Eingabemaske.

Spezielle Hardware für das KI-Training (TPUs oder GPUs) wird im ersten Projekt kaum erforderlich werden. Projektparameter, also die Anforderungen an das Ergebnis, sollten so überschaubar gewählt sein, dass ein Trainingslauf einer ML-KI in Stunden abgeschlossen wird. Die Hardware-Anforderung für ein kleines Projekt sollten gering ausfallen und der Bedarf einer trainierten KI im produktiven Betrieb ist nochmals deutlich niedriger als in der Trainingsphase, so dass ein gewöhnlicher Server ausreichen kann. Mit stabiler, sicherer Anbindung an die Behörde ist der Entwicklungsprozess gut für das Homeoffice geeignet.

Die zum Zeitpunkt dieses Textes mit Abstand populärsten Sprachen in der ML-Entwicklung sind *Python* für die Programmierung und *R* für statistische Analyse und Datenvorbereitung. Hier sind zahlreiche, ausgereifte Bibliotheken und mehrere Entwicklungsplattformen verfügbar. Viele Werkzeuge sind kostenfrei und können lokal implementiert werden. Für kommerzielle Produkte sind Abläufe für Ausschreibung und Beschaffung einzuplanen.

5. Besondere Abläufe bei einem KI-Projekt

Wir empfehlen, ML-Projekte oder andere KI-Verfahren nicht grundsätzlich anders zu betrachten als etablierte Software-Projekte, aber natürlich die spezifischen Besonderheiten zu berücksichtigen. Wir hoffen sehr, dass in absehbarer Zukunft ML-Anteile als eine eigene Phase oder ein Teilpaket in viele Software-Entwicklungsprojekte integriert werden, sobald grundlegende Erfahrungen mit KI-Projekten vorhanden sind.

Typische Aspekte für KI als Software wurden in Kapitel 3 angeführt und definieren besondere Kriterien für die Auswahl eines ersten Projektes. Es folgen noch einige Projekteigenschaften, die für KI-Projekte ins Gewicht fallen.

a) *Fail fast* – der Versuchscharakter

Es mag unter den verbreiteten behördlichen Vorgaben von mehrjährigen Planungszielen, Wirtschaftlichkeit der Mittel und den Karrierenachteilen eines Projektabbruchs unrealistisch erscheinen, aber ein erstes KI-Projekt sollte einen experimentellen Charakter haben. Der Rückstand von Digitalisierungsbemühungen in Behörden wird oft diskutiert und kritisiert, zu selten aber der Umfang regulatorischer Vorgaben, der mit der eigentlichen Geschwindigkeit der IT unvereinbar ist. Je nach Stand der etablierten Führungskultur kann es helfen oder nachteilig sein, auf das **erhöhte Risiko** hinzuweisen, dass ein erstes KI-Projekt nicht das erwartete Ergebnis liefert. Der Umgang mit dem Versuchscharakter ist eine Herausforderung an die Leitung des Behördenprojektes, weniger an Projektleiterin oder Projektleiter.

b) Iteration und Agilität

Ein häufiges Muster bei der KI-Entwicklung sind iterative Abläufe. Dies betrifft besonders die Entwicklung der Software, mit häufig variierten Rahmenparametern und angepassten Eingangsdaten. Aber es kann auch bei Tests oder im Betrieb häufiger erforderlich sein, eine laufende KI neu zu trainieren, wenn sich die Eingangsdaten verändert haben und die Ergebnisqualität sinkt.

Darüber hinaus sollte im Projekt das Risiko einkalkuliert werden, dass die KI die erwartete Abhängigkeit trotz intensiver Versuche nicht erfassen kann. Ebenso können ausgefallene Ergebnisse erzielt werden, wenn eine KI andere Abhängigkeiten herstellt, als im ursprünglichen Projektziel erwartet wurden. Es kann also auch sein, dass man das Projektziel aufgrund des Projektablaufs und der gesammelten Erfahrungen abändert.

Unter diesen Bedingungen wird deutlich, dass ein **agiler Projektablauf** besonders vorteilhaft für KI-Projekte ist.

c) Release-Ablauf und Reproduzierbarkeit

Für die iterativen Abläufe beim KI-Training ist es besonders effizient, einen möglichst weit automatisierten Prozess für **Release-Management** zwischen Software-Entwicklung und IT-Betriebsbereich zu etablieren.

Wie in Kapitel 4 erläutert, ist eine KI nur reproduzierbar, wenn der spezifische Software-Zustand aus Programmcode, Parametern und Eingangsdaten identisch ist. Für eine strukturierte Vorgehensweise und um etwa Fragen zum Datenschutz beantworten zu können, ist es daher empfehlenswert, versionierende **Repositorien** für alle Daten zu führen (sofern

keine regulatorischen Vorgaben dieser Speicherung entgegenstehen). Das umfasst gegebenenfalls auch synthetische Daten, sowie die Trainingssoftware und die eigentlichen, binären Programme. In einem so automatisierten Release-Ablauf lässt sich jede Entwicklungsstufe bei Bedarf nachvollziehen oder zurückrollen und ein späteres Re-Training im Betriebs-Lifecycle ist weniger aufwändig.

d) Schutzbedarfe, Sicherheit und Sensibilität der Daten und Entscheidungen

Wie im Abschnitt 3 angekündigt und diskutiert möchte NExT die Besonderheiten von Datenschutz, IT-Sicherheit und ethischen Aspekten der KI in der notwendigen Tiefe in einem separaten Whitepaper betrachten. Neuartig sind die Anforderungen für den Datenschutz zum Beispiel deshalb, weil sich Eingangsdaten unter bestimmten Bedingungen in abgeschwächter Weise aus einer trainierten KI rekonstruieren lassen. Auf der anderen Seite bedeuten automatisierte Abarbeitung und Prüfung von Daten durch eine Software in der Regel einen Gewinn für den Datenschutz, wenn der Zugriff auf Daten durch Menschen dadurch reduziert werden kann. Um das erste Projekt nicht mit Regulierungsfragen zu überfrachten, wiederholen wir unsere Empfehlung, möglichst gering personenbeziehbare Eingangsdaten zu wählen und sensible Bereiche zu vermeiden. Alle Verfahren sollten kommuniziert, abgestimmt und die erteilten Freigaben eingehalten werden. Für die IT-Sicherheit ist es vorteilhaft, das erste Projekt mit internen Mitarbeiterinnen und Mitarbeitern zu betreiben und damit rein hausintern ablaufende Prozesse zu verbessern. Wie in vielen Behördenprojekten wird ein nicht unwesentlicher Anteil der Projektlaufzeit auf diese Phase entfallen.

Problematisch kann für Behörden die Arbeit mit Cloud-Entwicklungsplattformen werden, die die führenden Anbieter für KI-Lösungen zu anfänglich sehr geringen Kosten offerieren. Diese Angebote sind Folge des Wettstreits um die populärste ML-Plattform und können ein KI-Projekt sehr vereinfachen. Aufgrund der Risiken für die Vertraulichkeit der Daten sind sie aber für den Behördeneinsatz grundsätzlich nicht geeignet, sofern keine veröffentlichten Daten genutzt werden. Über Cloud-Plattformen kann aus dem Homeoffice schneller begonnen werden, sie führen aber langfristig zur Anbieter-Abhängigkeit und können Projekte mit vertraulichen Inhalten verhindern. Es ist mit überschaubarem Aufwand möglich, die relevanten Elemente der populären Frameworks *on premise* zu installieren, die dann per VPN für die Entwickler erreichbar sind.

e) Internes Team und neue Rollen

Ein ML-Projekt benötigt zwei neue spezifische Rollen, die im vorangegangenen Kapitel 4 nur kurz aufgeführt wurden: **KI-Softwareentwickler** (4b) und ***data scientists*** (4c).

Der Begriff *data scientist*, der sich vor allem in datenintensiven Projekten etabliert hat, bezeichnet Experten für die softwaregebundene Analyse von meist großen Datenmengen. Sie sollten mit den spezifischen Eigenschaften der Daten vertraut sein und Fehler und Trends darin erkennen können. Wenn erforderlich, ist ein *data scientist* in der Lage, die Daten mit Software wie *R* rasch zu bearbeiten, zu filtern und zu visualisieren. *Data scientists* arbeiten im Projekt eng mit den Software-Entwicklern zusammen, die die KI trainieren, und können so die Ergebnisse der ML-Prozesse deutlich verbessern. In kleinen Projekten können beide Rollen auch von einer Person ausgefüllt werden.

Wenn eine Behörde ohnehin mit großen Datenmengen arbeitet, wird oft eine Organisationseinheit für diese oder ähnliche Aufgaben eingerichtet sein, etwa für statistische Analyse oder einen datenintensiven Fachbereich. Manchmal ist diese Funktion noch aus historischen Gründen über mehrere Einheiten verteilt. Erfolgversprechend ist der Ansatz, die Fertigkeiten und Kenntnisse in einer gesonderten Einheit zusammenzuführen und zu verstärken, zu Beginn auch experimentell in einem „Labor“ - ein Beispiel stellt der Bereich Fachanalytik im Bundesamt für Migration und Flüchtlinge dar. Für ein ML-Projekt kann es sehr wichtig sein, dass ein *data scientist* dauerhaft im Projekt aktiv ist und in der Organisationseinheit angesiedelt wird, die die Software entwickelt.

Auch für die eigentliche KI-Software-Entwicklung ist natürlich zu empfehlen, für diese besondere Expertise ein **festes, internes Team** aufzubauen. Dabei wird es sich als Vorteil erweisen, dass der Umfang der eigentlichen Software im ML überschaubar ist. Ein ML-Trainingsprogramm kann auf einige hundert bis wenige tausend geschriebene Zeilen Code beschränkt werden. Es ist also realistisch möglich, die Kenntnisse für interne Kräfte durch einige Wochen oder Monate Weiterbildung aufzubauen und ein Projekt dann intern durchzuführen. Dies ist auch in einem verteilten Team oder im Homeoffice möglich, wenn ausreichende Videokommunikationstechnik zur Verfügung steht.

Interne Entwicklung hat den Vorteil, dass die Kompetenz kontinuierlich zur Verfügung steht, um eine KI über die Zeit iterativ zu verbessern oder bei Bedarf ein Re-Training mit angepassten Eingangsdaten zu veranlassen; KI-Software ist weniger statisch als ein klassisches Produkt. Auch ist bei einem internen Team eine höhere Vertraulichkeit der Daten und bessere IT-Sicherheit zu erwarten.

Aufgrund der Personalsituation zum Zeitpunkt dieses Whitepapers ist es immer eine Herausforderung, interne oder externe Teams für ML zusammenzubringen oder zu beauftragen. Eine externe Beauftragung kann die Umsetzung eines Projektes natürlich beschleunigen oder, wenn die internen Ressourcen fehlen, sogar überhaupt erst ermöglichen. Wie bei allen externen Entwicklungsprojekten müssen Vertraulichkeit, Dokumentation und Rechteübertragung geklärt werden, damit die souveräne Kontrolle über alle Komponenten des Produktes in der Behörde bleibt und weitere Arbeit an der Software auch mit einem veränderten Team möglich ist.

Gerade wegen der starken Abhängigkeit von behördlichen Daten ist ein **interdisziplinäres Team vorteilhaft**, das die Fachbereiche einschließt. Eine offene und produktive Zusammenarbeit mit Gremien und Sachbearbeiterinnen und Sachbearbeitern, die in der Regel auch die späteren Anwender des Produktes werden, ist ein wichtiges Erfolgskriterium.

Abschließend soll nochmals daran erinnert werden, dass mit dem ersten KI-Projekt primär in Team und Behörde **Erfahrung gesammelt und Vorbehalte abgebaut** werden sollen. Die Projektleitung muss dies als wichtigen Teil der Aufgabe verstehen, den Projektablauf transparent gestalten und das Ergebnis offen kommunizieren, um so für Akzeptanz zu werben und mit den Vorteilen von *machine learning* zu überzeugen.