
Datenschutz, hybride IT und der Wille zur Innovation

FRANK OLTMANNS-MACK

Innovation, Digitalisierung und hybride IT – das sind die aktuellen Schlagwörter in der IT-Welt. Hybride IT gilt dabei als die einzige pragmatische Lösung, um den Fortbestand der Unternehmen in der Zukunft zu sichern. In Deutschland – und hier gerade auch im Mittelstand – wird der Datenschutz allerdings häufig als Argument ins Feld geführt, um hybride Lösungen abzulehnen und stattdessen an altbewährten Strukturen festzuhalten. Aber wie stichhaltig ist das Argument „Datenschutz“ wirklich? Oder liegen die Probleme nicht vielmehr an ganz anderen Stellen und der Datenschutz muss nur als Entschuldigung herhalten? Wie innovativen Lösungen zum Durchbruch verholfen werden kann, zeigen die „jungen Wilden“, wie z. B. FlixBus.

1. GESETZLICHE EBENE: NOTWENDIG, ABER UNZUREICHEND

Im Frühjahr 2016 hat die EU eine neue Datenschutz-Grundverordnung (DSGVO) verabschiedet, die ab Mai 2018 auch umgesetzt werden muss. Aufgrund dieser Tatsache haben der Deutsche Bundestag und der Deutsche Bundesrat 2017 ein Datenschutzgesetz beschlossen, welches das deutsche Recht den EU-Vorgaben anpassen soll.

Leider lässt sowohl die DSGVO als auch die Reform des deutschen Datenschutzgesetzes einiges zu wünschen übrig. Wichtige Themen der Digitalisierung werden vernachlässigt bzw. komplett ausgeklammert.

Dazu gehören ausgerechnet auch die Themen, die in Zukunft aller Voraussicht nach riesige Markttreiber sein werden, wie z. B.:

- Big Data
- Künstliche Intelligenz
- Ubiquitous Computing
- Smart Cars
- Smart Health
- Industrie 4.0

Neben der Vernachlässigung solch brisanter Themen krankt das neue Datenschutzgesetz daran, dass viele Vorgaben nur sehr oberflächlich präzisiert wurden und somit viel Spielraum für ihre Auslegung lassen. Und genau dieser Spielraum ist einer der Gründe, warum viele Unternehmen in Bezug auf den Datenschutz ausgesprochen risikoavers reagieren.

Ein Beispiel, mit dem der akute Konkretisierungsbedarf veranschaulicht werden kann, ist die Anwendung des Informationsrechts beim Internet der Dinge (Internet of Things – IoT). IoT ist darauf ausgerichtet, Sensordaten zu erfassen, zu verarbeiten und möglichst transparent einen Mehrwert zu liefern. Das ist jedoch problematisch im Hinblick auf das Informationsrecht, das die DSGVO einräumt, denn: Die Sensoren besitzen in der Regel kein Ausgabemedium, bei dem ein User, dessen Daten erfasst wurden, die entsprechenden Informationen abrufen kann. Im Fall des IoT gewährt die DSGVO den Nutzern also ein Recht, das die Betroffenen gar nicht wahrnehmen können, weil die technischen Voraussetzungen dafür nicht gegeben sind.

Im Übrigen ist die Geltung der DSGVO-Anforderungen sehr weitreichend und allgemein: Der Kiosk-Besitzer um die Ecke, der noch mit papiergebundenen Daten arbeitet, muss diesen Anforderungen genauso gerecht werden wie Amazon, Google oder Microsoft – internationale Großkonzerne, die über Data Lakes von gigantischem Ausmaß verfügen.

Zwischen den Interessen der Wirtschaftsunternehmen und der Politik zeigt sich häufig ein Bruch: Viele Gesetze erscheinen wenig praktikabel und adressieren kaum die Probleme der Unternehmen. Gerade in Bezug auf die DSGVO sollte der Gesetzgeber nachbessern und Lücken schließen. Prof. Dr. Alexander Roßnagel, Rechtswissenschaftler mit dem Schwerpunkt Recht der Technik an der Universität Kassel, bringt es auf den Punkt: „Das wirklich Interessante ist aber das, was nicht im Gesetz steht. Man hat hier viele Chancen nicht ergriffen“ [Ingo Dachwitz, netzpolitik.org, 2017]. Aber nicht nur die Gesetzeslage stellt einen großen Hemmfaktor dar für die Entwicklung innovativer Lösungen. Auch die soziale Ebene muss in Betracht gezogen werden.

2. SOZIALE EBENE: INNOVATION BRAUCHT DIE PASSENDE KULTUR

Aufgrund der mangelhaften Genauigkeit der Gesetze fühlen sich viele Mitarbeiter so überfordert und verunsichert, dass sie Veränderungen schlichtweg ablehnen. Lieber halten sie an altbekannten Mustern fest und versuchen, den Status Quo zu erhalten. Das alte Ideal der eigenen, abgeschotteten IT-Infrastruktur hinter der möglichst unüberwindbaren Mauer (Firewall) gilt auch heute noch vielerorts als das sicherste Modell. Um Innovationen – wie z. B. einer hybriden IT – den Weg zu bahnen, muss diese Denke allerdings aufgebrochen werden. Andere, flexiblere Konzepte bieten die gleiche Sicherheit. Gleichzeitig muss sich in den Unternehmen auch auf sozialer Ebene einiges ändern. Das hierarchische Modell der Unternehmensführung erweist sich vielfach als äußerst effektive Innovationsbremse. Führungspyramiden und die starren Prinzipien von Delegation und Verantwortung sind ungeeignet, um innovatives Denken zu fördern. Innovation erfordert Kreativität und Freiraum und sollte nicht durch umständliche Genehmigungsprozesse belastet werden.

John P. Kotter, Professor für Führungsmanagement an der Harvard Business School, erkannte dieses Problem schon 2012 [John P. Kotter, hbr.org, 2012]. Seiner Meinung nach müssen sich Unternehmen in zwei Bestandteile aufspalten: einen hierarchischen und einen agilen Teil. Der hierarchische Teil sichert, Kotters Modell zufolge, das mehr oder minder traditionelle Tagesgeschäft des Unternehmens und der agile Teil – den Kotter Netzwerk nennt – fördert die Innovation. Dabei ist die Kommunikation zwischen dem hierarchischen und dem agilen Unternehmensteil von großer Bedeutung, denn nur durch den konstanten Austausch gelingt es, bestehende Prozesse zu optimieren. Kotter identifiziert fünf Kernprinzipien:

1. Viele Change-Agenten, nicht nur die üblichen wenigen Ernannten
2. Eine positive Veränderungseinstellung
3. Kopf und Herz und nicht nur Kopf
4. Mehr Führung, aber nicht mehr Management
5. Zwei Systeme, eine Organisation

Die fünf Prinzipien bilden die Leitlinien für acht Prozesse, die das Innovationsmanagement vorantreiben:

1. Erzeugen Sie ein Gefühl der Dringlichkeit für eine einzelne große Opportunity.
2. Erschaffen und pflegen Sie zielgerichtete Zusammenarbeit

3. Formulieren Sie eine strategische Vision und entwickeln Sie Veränderungsinitiativen, um die große Opportunity zu nutzen
4. Kommunizieren Sie die Vision und die Strategie, um die Mitarbeiter zu integrieren und eine wachsende Freiwilligenarmee zu rekrutieren
5. Beschleunigen Sie die Entwicklung in Richtung Vision und Opportunity, indem Sie sicherstellen, dass das Netzwerk Hindernisse beseitigt
6. Feiern Sie sichtbare, signifikante kurzfristige Gewinne
7. Lassen Sie niemals nach. Lernen Sie aus Ihren Erfahrungen fortlaufend weiter. Erklären Sie den Sieg nicht zu früh
8. Institutionalisieren Sie strategisch kulturelle Veränderungen

Um nach den fünf Kernprinzipien zu handeln und die acht strategischen Prozesse umzusetzen, werden engagierte Mitarbeiter gebraucht. Nicht jeder Mensch ist dafür geeignet, innovativ zu denken und zu arbeiten. Eine Mindestanzahl veränderungsbereiter Kollegen wird jedoch benötigt, um Innovationen erfolgreich zu etablieren.

3. KOMPETENZEbene: DATEN & TECHNIK

Entscheidend für die Förderung von Innovation im Unternehmen sind weiterhin zwei Kernkompetenzen: Datenkompetenz und technische Kompetenz. Datenkompetenz umfasst das Wissen über Daten und ihre Verarbeitung. Zur technischen Kompetenz gehört die Fähigkeit, Software-Lösungen im Unternehmen effektiv und funktional einzusetzen. In beiden Kompetenzfeldern gibt es spezifische Herausforderungen.

3.1 DATENKOMPETENZ: KLASSIFIZIERUNG IST DAS ZAUBERWORT

Viele Unternehmen können heute nicht mehr entscheiden, welche ihrer Daten schutzwürdig sind und welche nicht. Deswegen wird im Hinblick auf den Datenschutz immer der maximal restriktive Ansatz gewählt: ALLE Daten müssen geschützt werden. Diese Entscheidung bedeutet das Aus für den Einsatz hybrider Modelle, die in der Kombination mit diesem maximal restriktiven Schutz zwangsläufig Datenschutzvorfälle provozieren.

Um diese Klippe zu umschiffen, müssen Daten klassifiziert werden, so dass zwischen geistigem Eigentum (Intellectual Property – IP) und weniger sensiblen Daten unterschieden werden kann. Aus zwei Gründen sind viele Unternehmen nicht bereit, diese Klassifizierung durchzuführen: Es fehlt an Know-how

– also an Datenkompetenz – und am Entschluss, in die notwendige Fähigkeit zur Datenklassifizierung zu investieren. Aber nur sauber klassifizierte Daten können sauber separiert und in hybriden Modellen an den richtigen Stellen gesichert werden. Durch die Abkapselung der kritischen Daten kann zusätzlich ein Skalierungseffekt – d. h. Flexibilität im Hinblick auf die notwendige Größe der Plattform – erzielt werden. Diese Entkopplung hilft auch dabei, zukünftige Datenschutzvorfälle zu vermeiden, da klar dokumentiert ist, welche Daten sich an welchen Stellen befinden. Dadurch wird insgesamt ein besserer Schutz unternehmenskritischer Informationen erreicht.

Das Wissen über die Daten ist in den Unternehmen meist stark fragmentiert. Die einzelnen Fachbereiche oder Abteilungen haben in der Regel Zugriff auf ihre eigenen Daten und wissen, wo bestimmte Informationen gesucht und gefunden werden können. Zugleich sind jedoch die Methoden der Datenspeicherung von Bereich zu Bereich unterschiedlich und es fehlt der allgemeine Überblick. Hier gilt es, eine zentrale Schaltstelle einzurichten, die über eine fundierte Datenkompetenz verfügt und auf dieser Basis einheitliche und allgemein verbindliche Vorgaben und Methoden definiert.

3.2 TECHNISCHE KOMPETENZ: WEITERBILDUNG UND -ENTWICKLUNG

Um die Leistungsfähigkeit eingesetzter Tools auch im Hinblick auf Sicherheit beurteilen zu können, fehlen häufig die entsprechenden Weiterbildungen der Anwender. Auch in der hybriden Welt gibt es sichere und geprüfte Methoden, um ausgelagerte Daten zu schützen. Allerdings führt die Unkenntnis dieser Methoden dazu, dass die Bereitschaft zum Einsatz sehr gering ist und viele sinnvolle Möglichkeiten ungenutzt bleiben. Fühlt sich die interne IT überfordert, dann strahlt diese Verunsicherung in das gesamte Unternehmen aus und es wächst eine generelle Ablehnung. Hier kann die Zusammenarbeit mit externen Partnern hilfreich sein: Durch den Einsatz von Best Practices können Hemmschwellen überwunden und Zutrauen gewonnen werden.

Ein weiterer Aspekt ist die interne Weiterbildung. Jedes Unternehmen muss für jede Mitarbeiterin und jeden Mitarbeiter einen Ausbildungsplan erstellen, der ausgerichtet ist an den Anforderungen der Firma und den Interessen und Bedürfnissen der Mitarbeiterin/des Mitarbeiters. Im Hinblick auf den Datenschutz gilt dies nicht nur für die interne IT-Abteilung, sondern auch für jede einzelne Fachabteilung: Datenschutz im Unternehmen ist weit davon entfernt, ein spezifisches IT-Thema zu sein. Das Bewusstsein für

den angemessenen Umgang mit Daten muss unternehmensweit geweckt werden. Die User müssen die Chance erhalten, Schritt zu halten und ihr Wissen der rasanten technischen Entwicklung anzupassen. Es ist eine Binsenweisheit, die nicht oft genug wiederholt werden kann: Die Akzeptanz neuer Technologien und Tools wächst, je gründlicher die User trainiert werden und je zuverlässiger sie Unterstützung erfahren. Wer hier spart, spart am falschen Ende.

Viele Softwareanbieter investieren sehr viel Geld in die Weiterentwicklung ihrer Produkte und legen dabei einen Schwerpunkt auf die Verbesserung der Sicherheit und auf die Implementation von Funktionalitäten, die DSGVO-Konformität ermöglichen. Leider entscheiden sich viele Unternehmen, lieber selbst entwickelte und damit schwer administrierbare Lösungen einzusetzen, anstatt ein fertiges Produkt zu kaufen. Investitionen zur Ablösung veralteter Lösungen werden gescheut. Dadurch wird das Sicherheitsrisiko im Lauf der Zeit immer größer und unberechenbarer. Für hybride IT-Lösungen sind solche Ansätze in den meisten Fällen ebenfalls ungeeignet. Innovative Lösungen erfordern ein innovatives Design.

4. TECHNISCHE EBENE: DAS RICHTIGE TOOL FÜR DIE RICHTIGE AUFGABE

Grundlegend für die Digitalisierung und hybride IT-Lösungen ist auch die Wahl der passenden Tools. Werden nicht die passenden Lösungen eingesetzt, so hemmt dies den ganzen Prozess und Impulse aus den anderen vorher genannten Bereichen verpuffen komplett. In Abgrenzung zu der technischen Kompetenz geht es in diesem Fall nicht um die Weiterbildung und das Wissen über den Einsatz der Anwendungen, sondern um die Tools selber. Wie ein Klempner die jeweils richtige Zange benötigt, so muss ein Mitarbeiter in der IT auch das richtige Werkzeug an die Hand bekommen.

Ein Unternehmen muss den Mitarbeitern die richtigen Tools und die richtige Infrastruktur zur Verfügung stellen, damit eine hybride IT bzw. neue innovative Ideen umgesetzt werden können. Außerdem muss der Raum für einen ständigen Wissensaustausch geschaffen werden, damit nicht einzelne Experten herangezogen werden, sondern die Kompetenzen im Unternehmen auf breiter Front wachsen. Dafür sollten Unternehmen unbedingt in kompetente Collaboration Tools investieren. Viele aktuelle Produkte haben den Wissensaustausch der Mitarbeiter im Fokus und adressieren genau die genannten Probleme. Leider fehlt oft der Überblick über die

vorhandenen Produkte. Dabei existieren heute schon leistungsfähige Tools, die sogar helfen, die aktuellen Compliance-Vorgaben einzuhalten. Zu diesem Zweck untersuchen die Anwendungen die Situation in der Infrastruktur und machen Vorschläge, wie bestimmte Mängel behoben werden können. Zusätzlich müssen die vorhandenen Daten sinnvoll gespeichert werden. Um die Daten zu schützen, reichen einfache Dateiablagen nicht mehr aus. Automatische Datenklassifizierung und Zugriffsrestriktionen sollten ebenso selbstverständlich genutzt werden wie sinnvolle Backup- und Disaster-Recovery-Möglichkeiten. Nur so kann sichergestellt werden, dass die Daten geschützt werden und zugleich hoch verfügbar sind.

5. ZUM BEISPIEL FLIXBUS

Ein Beispiel für eine unbelastete Herangehensweise an das Thema hybride IT bietet die Firma FlixBus aus München. FlixBus hat es in knapp fünf Jahren geschafft, die Spitze der Personentransportunternehmen in Europa zu erreichen: Der Marktanteil von Überlandbusreisen liegt mittlerweile bei mehr als 80 Prozent. Die Gründe für den großen Erfolg von FlixBus liegen zum einen in der Start-Up-Mentalität und dem damit verbundenen pragmatischen Ansatz bezüglich Datenschutz und hybrider IT, zum anderen aber auch in den Angeboten flexibler digitaler Dienste, wie z. B. Mobile Booking und Ticketing. Kombiniert sind diese Services mit einer dynamischen Preisgestaltung, die sich stark an Kapazität und Nachfrage orientiert. FlixBus hat sich – wie andere erfolgreiche Unternehmen – im Vorfeld mit allen angesprochenen Fragen und Herausforderungen intensiv auseinandergesetzt – und dann das Geschäftsmodell überlegt und unvoreingenommen komplett auf hybride IT ausgerichtet. Dazu gehören selbstverständlich die genaue Datenklassifizierung und der Einsatz effektiver Tools zum Datenschutz.

Bei der konsequenten Verfolgung einer Cloud-First-Strategie setzt FlixBus auf cloudbasierte Datenanalysen, um den Erfolg der 250 Regionalpartner zu maximieren. Dafür wurden spezifische Services entwickelt, die die Ertragssteuerung (FlixYieldr), das Auftragsmanagement und Booking (FlixCenter) sowie die Nachverfolgung der Busse (FlixTrackr) unterstützen. Auf technischer Ebene nutzt FlixBus eine vollständig vernetzte hybride Umgebung, in der Mitarbeiter, Unternehmensstandorte, Clouds und Daten effizient, sicher und kostengünstig miteinander verwoben sind. Der Einsatz von Public Cloud Computing ermöglicht eine hohe Flexibilität und hilft bei der Steigerung des Geschäftswachstums.

FlixBus hatte nicht mit Altlasten aus der Vergangenheit zu kämpfen und konnte von Grund auf neu auf der „grünen Wiese“ planen. Dadurch gelang es dem Unternehmen, viele alteingesessene Konkurrenten komplett vom Markt zu verdrängen, die die oben genannten Defizite hatten. Und diese Verdrängung werden viele Unternehmen in anderen Bereichen in den nächsten Jahren auch erleben, wenn sie nicht umdenken und die neuen technischen Möglichkeiten nutzen.

6. AUSBLICK & FAZIT

Die Digitalisierung lässt sich nicht aufhalten, und niemand kann verlässlich vorhersagen, wohin uns diese Transformation noch führen wird. Vorfälle, wie bei Facebook und Cambridge Analytica, sind die Folgen unklarer Gesetzesformulierungen, fehlender Richtlinien und der Passivität der beteiligten Parteien. Die deutsche Wirtschaft kann sich Passivität nicht leisten, da sie sonst vom Weltmarkt abgehängt wird. Die USA und China sind übermächtige Konkurrenten und weit voraus in der Entwicklung Künstlicher Intelligenz und datengestützter Analysen.

Es ist entscheidend, dass in Bezug auf den Datenschutz ein Umdenken erfolgt: Unternehmen und Politik müssen auf den genannten Ebenen dringend nachbessern – und dies sollte im Dialog geschehen. Es müssen klare Grenzen geschaffen werden und Unklarheiten beseitigt werden.

Gleichzeitig müssen sich die Unternehmen auch intern viel stärker aufstellen. Nur so können Impulse fruchtbar gemacht und der zukünftige Bestand gesichert werden. Im März 2018 äußerte sich der französische Präsident Emmanuel Macron in einem Interview zu den Aufgaben der Politik angesichts der Entwicklung von Künstlicher Intelligenz. Er forderte die „interdisziplinäre Kreuzung aus Mathematik, Sozialwissenschaften, Technologie und Philosophie. Das ist absolut kritisch.“ [Nicholas Thompson, Wired.com, 2018].

Sozialwissenschaftliche und philosophische Aspekte werden gerade in Deutschland in den letzten Jahren kaum berücksichtigt. Dabei sind auch sie ein essenzieller Bestandteil der Diskussion in Bezug auf die neuen Technologien und das Thema Datenschutz. Grundlegend ist z. B. die Frage, was Maschinen entscheiden dürfen und wo der Mensch unbedingt die letzte Entscheidungsgewalt behalten soll.

Zugleich müssen die Unternehmen den Mitarbeitern die Möglichkeiten bieten, sich auf Veränderungen auf Technik-, Kompetenz- und Unternehmenskulturebene vorzubereiten und eigene Ideen einzubringen. Datenschutzbeauftragte, die Angst haben, Fehler zu begehen oder gesetzliche Vorgaben falsch auszulegen, sind eher Bremser als Treiber der digitalen Transformation – und damit auch des mittel- und langfristigen Unternehmenserfolgs. Die mehr oder minder komplette Blockade von hybriden IT-Lösungen, Clouds oder der Nutzung von Künstlicher Intelligenz hilft auf die Dauer nicht weiter. Gesetzeslücken oder unklare Formulierungen dürfen nicht zum Stillstand führen. Der Wille und die Energie, innovativen Lösungen zum Durchbruch zu verhelfen, verdienen jede Unterstützung. Andernfalls drohen eine Stagnation der technischen Entwicklung und damit auch der Wegfall vieler Jobs. Viel Zeit ist schon verloren. Angst ist ein schlechter Ratgeber. Und die – in vielen Fällen unbegründete – Angst vor der Innovation erst recht.

QUELLEN

[John P. Kotter, hbr.org, 2012]:
<https://hbr.org/2012/11/accelerate>

[Ingo Dachwitz, Netzpolitik.org, 2017]:
<https://netzpolitik.org/2017/chance-verpasst-interview-zum-neuen-datenschutzgesetz/>

[Nicholas Thompson, Wired.com, 2018]:
www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/



FRANK OLTMANNS-MACK ist seit 2016 Consultant bei ORBIT Gesellschaft für Applikations- und Informationssysteme mbH in Bonn. Während und nach seiner Ausbildung als Diplom-Informatiker arbeitete er knapp 15 Jahre bei T-Systems als Cloud Consultant und -Architekt. Bei ORBIT hat der Experte seinen Fokus auf das Thema Cloud gelegt.

FRANK.OLTMANNS-MACK@ORBIT.DE • WWW.ORBIT.DE