

## Einleitung

In den letzten Jahrzehnten hat sich die Informationstechnologie wesentlich verändert. Konnten wir uns beispielsweise vor 20 Jahren noch nicht vorstellen, dass Medienangebote *on demand*, also auf unmittelbare Nachfrage, bereitgestellt werden, ist es heute normal, dass in einem Haushalt mehrere Personen unterschiedliche Inhalte streamen. Die *Cloud* ist heute überall, immer verfügbar und auf allen Endgeräten. Häuser werden nicht mehr verdrahtet, sondern es reicht aus, Funknetze zu bilden. Aber was ist der Preis? Der neue Funklautsprecher hört immer mit bei allen Gesprächen, die in seiner Umgebung stattfinden. Spätestens, seit in den USA ein großer Anbieter verpflichtet wurde, die Aufzeichnungen seines Lautsprechers für ein Gerichtsverfahren zur Verfügung zu stellen, wissen wir, dass Orwell mit seinem Werk »1984« der visionäre Elon Musk seiner Zeit war.

Nun gilt es, als Unternehmen den Spagat zu finden zwischen der Volldigitalisierung mit einer weitreichenden Optimierung, aber komplett neuen Risiken und einem eher konservativen, risikoaversen Ansatz, der versucht, die Risiken der Digitalisierung in Schach zu halten. In Horrorberichten liest man selbst von Universitäten, die zweistellige Millionenbeträge an Hacker zahlen, nur um ihre eigenen Daten wieder nutzen zu dürfen. Oder von Consulting-Firmen, die ihren kompletten Notebook-Bestand wegen Unbenutzbarkeit durch ein Computervirus oder eine Verschlüsselungsanwendung austauschen müssen. Es zeigt sich einerseits, dass die Digitalisierung nicht aufgehalten werden kann, aber andererseits stehen nun ganz andere Vertriebs- und Vermarktungsmöglichkeiten zur Verfügung.

Im Bereich der Geschäftsanwendungen hat Marktführer SAP den Weg in die Cloud für Großunternehmen mit Anwendungen aus dem Bereich Personalwirtschaft begonnen. *SAP SuccessFactors* und *SAP Concur* haben als Lösungen für die Verwaltung von Personalstammdaten und die Reisekostenabrechnung den Anfang gemacht. Damit wurden einerseits besonders schützenswerte Daten, aber wenig geschäftskritische Prozesse in die Cloud gehoben. Das hat dazu geführt, dass oftmals sensibelste, aber geschäftlich verhältnismäßig unkritische Daten in der Cloud verarbeitet wurden.

In den späten 1990er und frühen 2000er Jahren hat sich die Industrie mit *Outsourcing* bzw. *Outtasking* beschäftigt. Fragestellung war damals, ob man seine Systeme selbst hostet und wer Routineaufgaben übernimmt. Später war die Virtualisierung der Rechenzentren Thema. Man sprach nicht mehr von *Servern*, sondern nur mehr von *virtuellen Instanzen*, die man zwischen Sao Paulo, Los Angeles und Frankfurt nach Belieben hin- und herschieben konnte.

Neue Risiken der IT

Umgang mit schützenswerten Daten

**Cloud vs. on premise** Heute spricht man von *Cloud vs. on premise* und muss damit ganz ähnliche Entscheidungen in anderem Kontext treffen. Hebe ich die Datenbank in die Cloud, oder nutze ich einen Service? Welche Komponenten verbleiben on premise? Da oftmals nicht mehr transparent ist, wo die Daten genau liegen, ist es vielleicht doch nötig, etwas mehr Dokumentationen als üblich anzulegen. Es stellt sich die Frage, ob man in der Cloud noch selbst Verantwortung übernehmen muss. Oder läuft man dem Cloud-Service hinterher? Wie sicher ist es, sich auf einen Telekommunikations-Provider zu verlassen? Welche Sicherheitsrisiken geht man in Bezug auf Daten, Prozesse, Betriebsgeheimnisse etc. ein?

In diesem Zusammenhang kann nur wiederholt werden, was immer wieder gesagt wird: Die Lösungen, die ausgearbeitet werden, werden in der Regel von den Fachabteilungen beauftragt oder zumindest von den Fachabteilungen genehmigt. Wenn es um Sicherheit und Berechtigungen geht, kann man als IT-Verantwortliche\*r zuarbeiten, doch die Verantwortung für die Prozesse bleibt bei den Fachabteilungen, die den Mehrwert einer cloudbasierten Lösung gegen die Anforderungen und Risiken abwägen müssen.

Dieses Buch soll Ihnen dazu sowohl als Inspiration als auch als Anleitung dienen. Wir möchten die richtigen Fragen stellen und Empfehlungen daraus ableiten. Auch wenn es ein Buch von Technikern für Techniker\*innen ist, versuchen wir immer wieder einen Blick über den Tellerrand.

**Zielgruppen** Wir richten uns mit diesem Buch gleichermaßen an technikaffine Einsteiger\*innen in die SAP-Cloud und Profis. Sollten Sie gerade vor Ihrem ersten Cloud-Projekt stehen, finden Sie sicherlich passende Informationen. Fachlich richtet sich das Werk vornehmlich an IT-Administrator\*innen. Aber auch Entwickler\*innen finden hilfreiche Tipps zu relevanten Cloud-Services. Interessierte Personen aus den Fachabteilungen, die gerne über ihren Tellerrand schauen oder beispielsweise eine eigene Risikobewertung treffen wollen, werden ebenfalls fündig werden.

**Der Aufbau des Buches**

Wir beginnen dieses Buch mit der Positionierung von SAP und seiner Strategie im Kontext von Cloud-Produkten, um anschließend die SAP Business Technology Platform (SAP BTP) als PaaS-Angebot (Plattform as a Service) von SAP detailliert vorzustellen und ihre Sicherheitsaspekte zu beleuchten. Wir betrachten dann die Verbindungen zwischen der Cloud und Ihren Unternehmensnetzwerken, bis wir uns schließlich der Administration und Absicherung einzelner Cloud-Services widmen.

**Checklisten** Die meisten Kapitel schließen mit einer Checkliste ab. Anhand der Checklisten können Sie überprüfen, ob Sie die richtigen Fragen zu Ihrer hybriden

Systemlandschaft gestellt haben, und Themen gegebenenfalls noch einmal von einer anderen Seite durchdenken. Außerdem können Sie überprüfen, ob Sie beim Lesen des jeweiligen Kapitels alle wichtigen Inhalte verstanden haben. Wenn Sie beispielsweise die Neo-Umgebung der SAP BTP schon kennen, können Sie auch zuerst die entsprechende Checkliste durchgehen und so feststellen, ob das zugehörige Kapitel für Sie lesenswert wäre.

Wir stellen die Checklisten auch im Download-Bereich dieses Buches zum Herunterladen und Ausdrucken zur Verfügung. Sie finden sie auf der Seite [www.sap-press.de/5262](http://www.sap-press.de/5262) im Bereich **Materialien**.

Am Ende der meisten Kapitel finden Sie außerdem Praxisszenarien, in denen wir häufige Anforderungen Schritt für Schritt durchgehen. Diese Beispiele dienen der weiteren Vertiefung und können am eigenen System ausprobiert werden.

In hervorgehobenen Informationskästen finden Sie in diesem Buch Inhalte, die wissenswert und hilfreich sind, aber etwas außerhalb der eigentlichen Erläuterung stehen. Damit Sie diese Informationen sofort einordnen können, haben wir die Kästen mit entsprechenden Symbolen gekennzeichnet:

- In Kästen, die mit diesem Symbol gekennzeichnet sind, finden Sie Informationen zu *weiterführenden Themen* oder wichtigen Inhalten, die Sie sich merken sollten. 
- Dieses Symbol weist Sie auf *Besonderheiten* hin, die Sie beachten sollten. Es *warnt Sie* außerdem vor häufig gemachten Fehlern oder Problemen, die auftreten können. 
- Die mit diesem Symbol gekennzeichneten *Tipps* geben Ihnen spezielle Empfehlungen aus unserer Projektpraxis, die Ihnen die Arbeit erleichtern können. 
- *Beispiele*, durch dieses Symbol kenntlich gemacht, weisen auf Szenarien aus der Praxis hin und veranschaulichen die dargestellten Funktionen. 

Im Folgenden stellen wir Ihnen die Inhalte der einzelnen Kapitel dieses Buches vor.

In **Kapitel 1**, »Einführung in die SAP Business Technology Plattform«, führen wir Sie in die SAP BTP und die damit verbundene Terminologie ein. Wir erklären die Struktur und Positionierung der Plattform und legen dabei besonderes Augenmerk auf die Relevanz und die Einordnung in die SAP-Produktstrategie. Abschließend stellen wir die Nutzungsoptionen vor.

**Kapitel 2**, »Sicherheit auf der SAP Business Technology Plattform im Überblick«, beginnt mit einer Einführung in die verschiedenen Sicherheitsmechanismen des PaaS-Angebots von SAP. Authentifizierungs- und Autorisierungsmöglichkeiten werden eingeführt. Dabei erläutern wir die Unter-

Praxisszenarien

Informationskästen

Kapitel dieses Buches

schiede zwischen den verschiedenen Umgebungen der SAP BTP. Abschließend zeigen wir Ihnen die Anlage von Benutzerkonten und Berechtigungen auf Ebene der Global Accounts.

In **Kapitel 3**, »Sicherheit und Berechtigungen in der Neo-Umgebung konfigurieren«, beleuchten wir die Sicherheitsfunktionen in der Neo-Umgebung der SAP BTP im Detail. Wir zeigen zunächst, wie man unterschiedliche Trust-Konfigurationen einrichtet. Anschließend erläutern wir die Verwaltung von Benutzern, Rollen und Benutzergruppen.

In **Kapitel 4**, »Sicherheit und Berechtigungen in der Cloud-Foundry-Umgebung konfigurieren«, erläutern wir Sicherheitsaspekte der Cloud-Foundry-Umgebung der SAP BTP. Anhand einer Best-Practice-Implementierung zeigen wir Ihnen, wie der Betrieb sicher und günstig gestaltet werden kann.

Das **Kapitel 5**, »Cloud Connector«, widmen wir uns dem *Cloud Connector*, der zur Verbindung von Cloud- und On-Premise-Systemen eingesetzt wird. Dabei handelt es sich um eine zentrale Komponente für den Aufbau hybrider Systemlandschaften. Nachdem wir die Architektur erläutert haben, finden Sie eine Anleitung zur Installation und Konfiguration des Cloud Connectors. Die Absicherung wird detailliert beschrieben. Abschließend zeigen wir die Einrichtung des *SAP Destination Service*, der das Gegenstück zum lokal installierten Cloud Connector in der Neo- und Cloud-Foundry-Umgebung der SAP BTP bildet.

In **Kapitel 6**, »Administrationswerkzeuge der SAP Business Technology Platform«, geben wir Ihnen Empfehlungen zur Administration der SAP BTP, um die Organisation nicht mehr als unbedingt nötig zu belasten. Wir stellen Ihnen Konsolenwerkzeuge und APIs vor, die eine effiziente Administration ermöglichen.

In **Kapitel 7**, »Sicherheitsaspekte wichtiger Cloud-Services«, möchten wir Ihnen einen Überblick über die unserer Einschätzung nach wichtigsten Services der SAP BTP geben und diese unter sicherheitstechnischen Gesichtspunkten betrachten.

Zusammenfassend haben wir versucht, ein möglichst rundes und vollständiges Bild der Sicherheitsthemen im Zusammenhang der SAP BTP zu zeichnen. Wir danken Ihnen für das Interesse an unserem Buch und wünschen Ihnen viel Vergnügen bei der Lektüre!

**Martin Koch und Siegfried Zeilinger**