Sicherheit von Cloud-basierten Plattformen zur Anwendungsintegration: eine Bewertung aktueller Angebote

Dr. Nico Ebert, Prof. Dr. Kristin Weber

Cloud-basierte Plattformen zur Anwendungsintegration versprechen die einfache und kostengünstige Integration zwischen Anwendungen in der Cloud und bestehenden „On-Premise"-Anwendungen. Sie bieten zahlreiche Anwendungsadapter und erlauben den grafischen Entwurf, die Ausführung und die Verwaltung von komplexen Integrationsprozessen in der Cloud. Allerdings sind sie sicherheitskritische Elemente innerhalb der IT-Architektur, da sie Zugriff auf unterschiedliche Anwendungen und Daten des Unternehmens haben können. Daher stellt sich die Frage, inwiefern notwendige Sicherheitsanforderungen durch die Anbieter Cloud-basierter Plattformen erfüllt werden. In diesem Artikel werden sieben ausgewählte Integrationsplattformen detaillierter betrachtet und anhand der Sicherheitsanforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bewertet.

Zusätzliche Schlüsselwörter: Cloud-basierte Integrationsplattform, Integration-Platform-as-a-Service, Sicherheitsanforderungen, Informationssicherheit, Datenschutz

1 EINLEITUNG

Eine Alternative zur direkten Anbindung zwischen Anwendungen und zu Enterprise-Application-Integration-Plattformen (EAI) sind Cloud-basierte Integrationsplattformen. Sie versprechen die Vorteile von Cloud-Lösungen (z. B. geringe Kapitalbindung, hohe Flexibilität, wenig erforderliches Betriebs-Know-how) in Kombination mit dem Nutzen von EAI-Plattformen (z. B. Reduktion der Schnittstellen-Anzahl durch zentralen Hub, standardisierte Anwendungsadapter). Das Schweizer Logistikunternehmen Kardex ist ein Beispiel für die Verwendung einer Cloud-basierten Integrationslösung, um ERP, SaaS und mobile Anwendungen zu integrieren [Boillat und Legner (2014)].

Da die Plattformen auf verschiedene Unternehmensanwendungen in der Cloud („SaaS") und innerhalb des Unternehmens („On-Premise") zugreifen und deren Daten zum Teil in der Cloud verarbeiten, stellen sich insbesondere Fragen nach Informationssicherheit und Datenschutz der Plattformen. Besonders kritisch ist die Anbindung der Bestandssysteme innerhalb

Dr. Nico Ebert
Schuberstrasse 9,
8037 Zürich, Schweiz

Prof. Dr. Kristin Weber
Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt,
Fakultät Informatik und Wirtschaftsinformatik,
Sanderheinrichsleitenweg 20,
97074 Würzburg
http//fiw.fhws.de

der Unternehmensinfrastruktur, weil potentielle Angreifer über die Plattform Zugriff auf diese Systeme erhalten könnten. Gleichzeitig sind die Einfluss- und Kontrollmöglichkeiten für die Nutzer der Plattformen aufgrund des „Plattform als Service" jedoch geringer als bei selbstbetriebenen EAI-Plattformen.

In diesem Artikel werden zunächst die Cloud-basierten Plattformen zur Anwendungsintegration vorgestellt (Kapitel 2). Die „Sicherheitsempfehlungen für Cloud Computing Anbieter" des Bundesamtes für Sicherheit in der Informationstechnik (BSI, Kapitel 3) bilden schließlich die Grundlage für die Bewertung von sieben ausgewählten Plattformen (Kapitel 4).

2 CLOUD-BASIERTE INTEGRATIONSPLATTFORMEN

Cloud-basierte Integrationsplattformen[1] zählen zu den „Platforms as a Service" (PaaS) [Tietz et. al. (2011)] und sind mandantenfähige Systeme, in denen sich verschiedene Kunden eine Systeminstanz teilen. Sie erlauben die Entwicklung, Ausführung und Verwaltung von Integrationsprozessen und die Verbindung von On-Premise- und SaaS-Anwendungen [Pezzini und Lheureux (2011)]. Der funktionale Fokus der Plattformen ist die Integration auf Daten- und Funktionsebene. Die Integration auf Ebene der Geschäftsprozesse z. B. über BPM-Komponenten wird nur selten abgedeckt, die Integration auf Ebene der Benutzeroberflächen ist nicht Bestandteil der Plattformen. Die Funktionsbausteine der Plattformen unterscheiden sich jedoch nicht von denen klassischer EAI-Plattformen [Ring (2000)]:

- Prozessmanagement: Die Prozessmanagement-Funktionalität dient der Ausführung der Transformationsoperatoren.
- Transformation: Verschiedene Operatoren erlauben z. B. die Abbildung zwischen unterschiedlichen Datenschemata und Datenformaten.
- Konnektivität: Vorgefertigte Adapter ermöglichen die Anbindung von Cloud- oder On-Premise-Anwendungen. Die Kopplungsmechanismen erlauben die Verknüpfung der Anwendungen über Dateitransfers, asynchrone Nachrichten und synchrone Dienstaufrufe.
- Administration und Entwicklung: Administrationsfunktionen sind z. B. das Deployment und Monitoring der Integrationsprozesse. Schließlich verfügen alle Plattformen über Entwicklungswerkzeuge, z. B. für die grafische Modellierung von Integrationsprozessen.

Generell können zwei Plattformarchitekturen unterschieden werden. Im ersten Fall erfolgt die Integration zwischen den beteiligten Anwendungen in der Cloud. Daten von lokalen wie SaaS-Anwendungen werden gleichermaßen an die Cloud der Plattform übertragen und dort verarbeitet. In der Cloud werden nur Metadaten gespeichert, das sind insbesondere Prozessmodelle, Datenstrukturen und -abbildungen sowie Konfigurationsdaten für Anwendungsadapter (z. B. Benutzername und Passwort). In diesem Fall liegt die Verantwortung für die Betreuung der Integrationsinfrastruktur vollständig beim Anbieter. Als Alternative zur Verarbeitung der Daten in der Cloud kann die Datenintegration auch lokal erfolgen. Dabei wird in der lokalen Umgebung durch den Nutzer eine spezielle Laufzeitumgebung („Software-Agent") installiert. Die Daten von SaaS und lokalen Anwendungen werden an die lokale Laufzeitumgebung übermittelt und dort verarbeitet. Integrationsdaten werden in der Folge nicht in die Cloud des Plattformanbieters transferiert. Zwischen lokaler Laufzeit und Cloud werden lediglich Metadaten ausgetauscht, die in der Cloud gespeichert werden. Erfolgt die Datenintegration lokal, ist das Unternehmen selbst für die Integrationsinfrastruktur (inkl. Lastverteilung) verantwortlich.

[1] Von [Pezzini und Lheureux (2011)] als „Integration Platform as a Service" (IPaaS) bezeichnet.

Unabhängig vom Architekturtyp erfolgt die Administration (z. B. Benutzerverwaltung oder Monitoring) über eine webbasierte Oberfläche der Integrationsplattform. Der Entwurf der Integrationsprozesse erfolgt – je nach Plattform – ebenfalls über eine Weboberfläche oder über eine lokale Anwendung, die den Upload der Prozesse zur Plattform erlaubt.

3 BEDROHUNGEN UND SICHERHEITSANFORDERUNGEN IM CLOUD-COMPUTING

Cloud-Computing-Systeme sind grundsätzlich komplexe verteilte Systeme, weswegen sie prinzipiell den hierfür geltenden Bedrohungen ausgesetzt sind. Diese sind z. B. Sicherheitslücken im System des Anbieters wie die mangelhafte Benutzerauthentisierung oder die fehlende Überprüfung von Benutzereingaben auf schadhaften Code. Da die Kunden jedoch physische Ressourcen nutzen, auf die sie selbst keinen unmittelbaren Zugriff haben, ergeben sich eine Reihe spezifischer Bedrohungen [Vossen u. a. (2012), S. 175-178]:

- Unüberprüfbare Datenhaltung: Die Datenhaltung liegt in der Hoheit des Anbieters oder dessen Zulieferer und ist in der Regel nicht durch den Kunden überprüfbar (z. B. endgültiges Löschen von Daten).
- Mangelhafte Kontrollmöglichkeiten über Anbieter: Protokolle und Dokumentationen zur Datenverarbeitung befinden sich beim Anbieter, weswegen Kontrollen in der Regel nur eingeschränkt möglich sind.
- Vervielfältigung und Verteilung der Daten: Kunden haben keine Gewissheit, wie Anwendungen bzw. Daten geographisch verteilt sind.
- Nichtverfügbarkeit von Diensten: Cloud-Anbieter nutzen häufig selbst Dienste anderer Cloud-Anbieter. Durch das Ineinandergreifen zahlreicher Dienste bekommt die Stabilität der jeweiligen Schnittstellen eine gesteigerte Bedeutung. Änderungen an einer grundlegenden API eines Anbieters können z. B. dazu führen, dass Dienste eines anderen Anbieters nicht mehr funktionieren. Das Schutzziel der Verfügbarkeit von Diensten und Daten ist bezogen auf den einzelnen Anbieter somit besonders gefährdet[2].
- Gesteigerte Komplexität der IT-Landschaft: Aufgrund der starken Verteilung von Cloud-Diensten sind sie insgesamt komplexer als klassische verteilte Systeme. So sind IT-Infrastruktur und das Betriebspersonal häufig global – auch über unterschiedliche Firmen – verteilt.
- Gegenseitige Beeinflussung der Nutzer: Da sich verschiedene Nutzer eine Plattform teilen, ist die gegenseitige Beeinflussung nicht ausgeschlossen (z. B. Zugriff eines Nutzers auf Daten eines anderen Nutzers).

Zur Gewährleistung der Informationssicherheit ist eine Reihe von technischen und organisatorischen Sicherheitsmaßnahmen erforderlich. Informationen bzw. Daten sind zu schützende Güter für die insbesondere die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität (d. h. Vollständigkeit und Unversehrtheit) gelten [Federrath und Pfitzmann (2000)]. Die technischen Sicherheitsmaßnahmen betreffen sowohl die Infrastruktur (Netzwerk, Hosts, Anwendungen) als auch die Daten. Dazu zählen z. B. Verschlüsselungsmechanismen für die Übertragung von Daten und Autorisierungsverfahren für Benutzer. Komplementär dazu sind organisatorische Maßnahmen wie Mitarbeiterschulungen oder die Schlüsselverwaltung [Vossen u. a. (2012), S. 180 ff.].

Verarbeiten die Cloud-Computing-Systeme personenbezogene Daten, wie es etwa bei CRM-Systemen in der Regel der Fall ist, müssen zudem die Regelungen zum Datenschutz be-

[2] Unter Umständen kann die Verfügbarkeit jedoch durch die Verteilung auf mehrere Anbieter oder die Spezialisierung der Infrastruktur-Zulieferer auch steigen.

achtet werden. Die datenschutzrechtlichen Anforderungen sind in Deutschland insbesondere durch das Bundesdatenschutzgesetz (BDSG) geregelt. Werden von einem Unternehmen die Daten von Personen, die unter das BDSG fallen, durch einen Dritten verarbeitet, muss der Betroffene dazu im Vorfeld auf freiwilliger Basis einwilligen und der Dritte muss seinerseits das BDSG beachten (§ 4c Abs. 1 BDSG). Findet die Datenverarbeitung jedoch im Rahmen einer Auftragsdatenverarbeitung im Geltungsbereich des BDSG bzw. der EG-Datenschutzrichtlinie statt, ist keine Einwilligung der Betroffenen erforderlich, da Auftraggeber und Auftragnehmer als eine rechtliche Einheit betrachtet werden [Gola und Schomerus (2015), S. 299]. Cloud-Computing wird als Auftragsdatenverarbeitung eingestuft [Gola und Schomerus (2015)].

Die Auftragsdatenverarbeitung setzt allerdings voraus, dass die Daten innerhalb der EU oder in Ländern verarbeitet werden, deren Datenschutzniveau von der EU-Kommission als angemessen betrachtet wird (z. B. in der Schweiz). Mit den USA als Drittstaat wurde von der EU ursprünglich das „Safe-Harbor"-Abkommen beschlossen, mit dem sich Anbieter gegenüber dem Handelsministerium zur Einhaltung von „vergleichbaren" Datenschutzprinzipien wie in der EU verpflichten können. Dieses Abkommen wurde jedoch vom Europäischen Gerichtshof als ungültig erklärt [EuGH (2015)]. Als Alternative zu „Safe-Harbor" können die US-amerikanischen Unternehmen in der Theorie jedoch „Standardvertragsklauseln" der EU zustimmen [vgl. EU Kommission (2015)], wie dies z. B. der CRM-Anbieter Salesforce.com unmittelbar nach dem EuGH-Urteil tat. Aus den datenschutzrechtlichen Anforderungen ergeben sich eine Reihe von Maßnahmen für die Anbieter, etwa die Bestellung eines Datenschutzbeauftragten oder die Kontrolle des Zugriffs auf die personenbezogenen Daten (§ 9 BDSG, § 4f Abs. 1 Satz 1 BDSG).

Die Anforderungen an Informationssicherheit und Datenschutz im Cloud-Computing wurden von unterschiedlichen Organisationen in Form von Empfehlungen und Standards zusammengefasst. Die internationale „Cloud Security Alliance", in der einige Kundenorganisationen, Anbieter und Universitäten organisiert sind, bietet mit der „Cloud Controls Matrix" einen Überblick über verschiedene Empfehlungen und Standards [CSA (2014)]. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt in seinem Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter" [BSI (2012)] Vorschläge betreffend Informationssicherheit und Datenschutz. Die verschiedenen Anforderungsbereiche sowie ausgewählte Beispielanforderungen für Public-Cloud-Anbieter zeigt Tab. 1. Unterschieden wird zwischen den Anforderungskategorien Basis (B), hohe Vertraulichkeit für Daten mit hohem Schutzbedarf für Vertraulichkeit (C+) und hohe Verfügbarkeit (A+) für Dienstleistungen mit hohem Verfügbarkeitsbedarf. Das Schutzziel Integrität wird nicht durch die BSI-Anforderungen abgedeckt.

[3] Daneben wird der Datenschutz für nicht-öffentliche Stellen auch durch das Telemedien- und das Telekommunikationsgesetz geregelt.

ANFORDERUNGSBEREICH	BEISPIELANFORDERUNG (B = Basis, C+ = hohe Vertraulichkeit, A+ = hohe Verfügbarkeit)
Sicherheitsmanagement beim Anbieter	(B) Implementation eines anerkannten Informationssicherheits-Managementsystems (z. B. ISO 27001)
Sicherheitsarchitektur Rechenzentrums-Sicherheit	(B) Überwachung des Zutritts: Zutrittskontrollsystem, Videoüberwachungssysteme, Bewegungssensoren, Sicherheitspersonal, Alarmsysteme, etc.
Serversicherheit	(C+, A+) Einsatz zertifizierter Hypervisoren (Common Criteria mindestens EAL 4)
Netzsicherheit	(B) Verschlüsselte Kommunikation zwischen Cloud Computing-Anbieter und -Nutzer (z. B. TLS/SSL)
Anwendungs- und Plattformsicherheit	(B) Sichere Isolierung der Anwendungen (PaaS)
Datensicherheit	(B) Regelmäßige Datensicherungen, deren Rahmenbedingungen (z. B. Umfang, Speicherintervalle) nachvollziehbar sind
Schlüsselmanagement	(B) Best-Practices der Schlüsselverwaltung umsetzen
ID- und Rechtemanagement	(C+) Starke Authentisierung (z. B. Zwei-Faktor-Authentisierung) für Cloud-Kunden
Kontrollmöglichkeiten für Nutzer	(B) Kunden müssen die Möglichkeit haben, messbare Größen, wie im SLA vereinbart, zu überwachen
Monitoring und Security Incident Management	(B) 24/7 umfassende Überwachung der Cloud-Dienste sowie zeitnahe Reaktion bei Angriffen bzw. Vorfällen
Notfallmanagement	(B) Der Anbieter muss ein Notfallmanagement betreiben
Portabilität und Interoperabilität	(B) Exit-Vereinbarung mit zugesicherten Formaten unter Beibehalten aller logischen Relationen und ggf. Offenlegung der damit verbundenen Kosten (SaaS)
Sicherheitsprüfung und -nachweis	(C+, A+) Regelmäßige und unabhängige Sicherheitsrevisionen
Personalanforderungen	(B) Sensibilisierung der Mitarbeiter des Cloud Service Anbieters für Informationssicherheit und Datenschutz
Vertragsgestaltung Transparenz	(B) Offenlegung der Subunternehmer des Anbieters
Service Level Agreements	(B) Definierte Sicherheitsleistungen durch Security-SLA oder im SLA deutlich hervorgehoben
Datenschutz/Compliance	(B) Gewährleistung des Datenschutzes nach dt. Recht (B) Für den Cloud-Nutzer relevante gesetzliche Bestimmungen müssen durch den Anbieter eingehalten werden

Tab. 1: Anforderungsbereiche für Public-Cloud-Anbieter gemäß den Sicherheitsempfehlungen des BSI (Auszug aus [BSI (2012), S. 22 ff.])

Abgeleitet von den genannten Bedrohungen können die im vorherigen Abschnitt genannten Anforderungen des BSI präzisiert werden:

- Sicherheitsarchitektur insb. Netzsicherheit: Für die Integration von On-Premise-Anwendungen sind Maßnahmen zu treffen, die den Schutz der gesamten IT-Landschaft gewährleisten. Denkbar sind z. B. die verschlüsselte Kommunikation zwischen Plattform und On-Premise-Anwendungen sowie Proxy-Dienste und dedizierte Sicherheitszonen als Zwischenschicht zwischen On-Premise-IT und Plattform [BSI (2012), S. 32 f.].
- Sicherheitsarchitektur insb. Schlüsselmanagement: Kritische Daten müssen verschlüsselt werden. Hervorzuheben sind Passwörter, die in den Anwendungsadaptern hinterlegt sind, um auf die Anwendungsschnittstellen zuzugreifen. Ein Schlüsselmanagement muss sicherstellen, dass die verwendeten Schlüssel vertraulich, integer und authentisch erzeugt, gespeichert, ausgetauscht, genutzt und vernichtet werden [BSI (2012), S. 39 ff.].
- ID- und Rechtemanagement: Für die Mitarbeiter des Plattform-Anbieters aber auch für die Nutzer der Plattform auf Kundenseite (z. B. Entwickler, IT-Architekten) muss eine starke Authentisierung (z. B. Zwei-Faktor-Authentisierung) genutzt werden. Zudem muss ein rollenbasiertes Rechtemanagement-System den Zugriff auf Integrations- und Metadaten auf Anbieter- und Nutzerseite regeln und protokollieren [BSI (2012), S. 43 ff.].

4 BEWERTUNG CLOUD-BASIERTER INTEGRATIONSPLATTFORMEN

4.1 Vorgehen

Zur Bewertung ausgewählter Cloud-basierter Plattformen wurden die Kriterien des BSI genutzt, weil angenommen wird, dass diese in Deutschland häufig Anwendung finden. Allerdings wurden sie um das Kriterium der Integrität erweitert. Eine Internetsuche mit Google nach „Integration Platform as a Service", „IPaaS", „Integration Platform" und „Cloud Integration" ergab 23 Plattformen, welche die in Kapitel 2 erwähnten Funktionalitäten aufwiesen. Hiervon wurden Dell Boomi Atomsphere, IBM Cast Iron Live, Informatica Cloud, Jitterbit, MuleSoft Cloudhub, SAP HCI und Snaplogic ausgewählt, denen das Marktforschungsunternehmen Gartner [Pezzini u. a. (2015)] im „magischen Quadranten" eine subjektiv besondere „Vollständigkeit der Vision" (u. a. Marktverständnis, Geschäftsmodell, Innovation) und „Fähigkeit zur Umsetzung" (u. a. Produktqualität, Kundensupport) zugewiesen haben. Die „magischen Quadranten" der Firma Gartner werden von Unternehmen in der Praxis häufig zur Auswahl von Software herangezogen. Daher kann davon ausgegangen werden, dass die gut im Quadranten positionierten Plattformen häufig in die Auswahl eingeschlossen werden. Nachfolgend wurden Testversionen[4], Produktbeschreibungen, Dokumentationen und Videos ausgewertet. Interviews mit den Herstellern wären im Rahmen der weiteren Forschung wünschenswert (z. B. zu internen Prozessen der Anbieter).

4.2 Sicherheitsmanagement beim Anbieter

Die betrachteten Anbieter verfügen über unterschiedliche Systeme zum Management der Informationssicherheit. Verbreitet ist die ISO 27001 [ISO (2013)] ebenso wie die „Service Organisation Controls 2" (SOC 2). Bei SOC 2 handelt es sich um einen amerikanischen Standard aus der Wirtschaftsprüfung, der auch Anforderungen an die Informationssicherheit umfasst [AICPA (2014)]. Allerdings ist aufgrund der unzureichenden Angaben der Anbieter unklar, was der Geltungsbereich dieser Zertifikate ist (z. B. nur Rechenzentrum) und ob das Sicherheitsmanagement alle Mitarbeiter und Systeme des Anbieters umfasst. Einige Anbieter halten sich zudem an branchenspezifische Standards zur Verarbeitung von Krankenversicherten-

[4] Die Testversion war bei IBM Cast Iron Live nicht verfügbar.

und Patientendaten wie den „Health Insurance Portability and Accountability Act“ (HIPAA), den „Health Level Seven International Standard“ (HL7) oder den „Health Information Trust Alliance Standard“ (HiTrust) sowie zur Verarbeitung von Kreditkartendaten den „Payment Card Industry Data Security Standard“ (PCI DSS). Zwar verweisen einige Hersteller (z. B. Dell) ebenfalls auf Zertifizierungen (z. B. ISO 27001), allerdings gelten diese zum Teil nur für die Cloud-basierte IT-Infrastruktur (z. B. Amazon). Die Zertifikate sagen nichts über die Sicherheitsstandards für die Entwicklung und den Anwendungsbetrieb der Integrationsplattform aus, die sich auf der IT-Infrastruktur befindet.

4.3 Sicherheitsarchitektur

4.3.1 Rechenzentrums-Sicherheit, Serversicherheit und Netzsicherheit

Mit Ausnahme von IBM und SAP nutzen die Anbieter Cloud-basierte IT-Infrastrukturen von Amazon oder Rackspace. Sämtliche Infrastrukturen verfügen über ein Sicherheitsmanagement basierend auf ISO 27001. Der Zugriff auf die Weboberfläche der Plattform (z. B. zur Administration) erfolgt bei allen Anbietern über eine verschlüsselte HTTPS/TLS-Verbindung. Alle Anbieter mit Ausnahme von Informatica ermöglichen die Ausführung der Integrationsprozesse in der Cloud. Der Zugriff auf lokale Anwendungen beschränkt sich in der Regel auf eine „demilitarisierte Zone“ (vgl. z. B. [Dell (2015)]) oder eine „Virtual Private Cloud“ (vgl. z. B. [MuleSoft (2015)]). Die Datenübertragung zwischen lokaler Umgebung und Integrationsplattform erfolgt im ersten Fall über eine gesicherte HTTPS- oder SFTP-Verbindung und im zweiten Fall über einen IPsec oder TLS gesicherten VPN-Tunnel.

Dell, IBM, Informatica, Jitterbit und Snaplogic unterstützen die lokale Ausführung der Integrationsprozesse. In diesem Fall verschlüsselt die lokale Laufzeitumgebung die Datenübertragung zur Cloud-Plattform (z. B. TLS 1.0 und TLS 1.2, vgl. z. B. [Dell (2015)]). Der lokale Laufzeit-Agent und die Plattform tauschen lediglich Status- und Metadaten aus. Die Anwendungsadapter der Plattformen unterstützen vielfältige Sicherheitsstandards zur Kommunikation mit den integrierten Anwendungen (z. B. WS-Security, OAuth2). SAP HCI erlaubt zudem die Verschlüsselung auf Nachrichtenebene via PKCS#7 sowie die Verschlüsselung von Dateitransfers via SFTP und PGP.

4.3.2 Anwendungs- und Plattformsicherheit

Die Plattformen sind durchgängig mandantenfähig, allerdings machen die Anbieter fast keine Angaben dazu, wie Mandanten voneinander isoliert werden. Lediglich SAP verweist auf separate Datenschemata [SAP (2013), S. 11 ff.]. Dell und Jitterbit weisen zusätzlich darauf hin, dass bei der Entwicklung die OWASP-Top10-Risiken von Webanwendungen berücksichtigt werden[5] [OWASP (2013)]. Mit Ausnahme von MuleSoft und SAP bieten die Anbieter lokale Laufzeitumgebungen für die Integration von On-Premise-Systemen. Diese haben den Vorteil, dass Integrationsdaten nicht mit der Cloud des Plattformanbieters ausgetauscht werden, sondern lediglich zwischen On-Premise- und SaaS-Anwendungen. Die Plattform in der Cloud tauscht mit der lokalen Umgebung lediglich Metadaten über eine HTTPS-Verbindung aus.

[5] Dazu zählen z. B. das „Cross-Site-Scripting“ oder die „Code-Injection“.

Tab. 2: Bewertung ausgewählter Cloud-basierter Integrationsplattformen anhand der BSI-Anforderungsbereiche (Quelle: Eigene Darstellung)

Kriterium	Dell Boomi Atomsphere	IBM Cast Iron Live	Informatica Cloud	Jitterbit	MuleSoft Cloudhub	SAP HCI	Snaplogic
4.2 Sicherheitsmanagement beim Anbieter	k. A.	ISO 27001 (unklar, ob nur RZ)	ISO 27001, PCI DSS	HIPAA/HL7	SOC 2, PCI, HiTrust	ISO 27001:2013, Cobit, SOC 2, PCI, ISF	SOC 2
4.3 Sicherheitsarchitektur							
a. RZ-/Server-/Netzsicherheit	ISO 27001:2005, SCO 1 (Rackspace), 128-Bit-SSL für Weboberfläche/ On-Premise-Anbindung, Adapter mit versch. Standards (z. B. WS-Security)	ISO 27001 (eigene RZ), SSL für Weboberfläche/ Agenten, Adapter mit versch. Standards (WS-Security)	ISO 27001/2 (Amazon), 128-Bit-SSL für Weboberfläche/On-Premise-Anbindung, Adapter mit versch. Standards (z. B. WS-Security)	ISO 27001/2 (Amazon AWS), SSL für Weboberfläche/Agenten, Adapter mit versch. Standards (WS-Security)“	ISO 27001/2 (Amazon), 128-Bit-SSL für Weboberfläche, VPC für On-Premise-Anbindung, Adapter mit versch. Standards (z. B. OAuth2)	eigene Infrastruktur, D/ USA, ISO 27001, SSL für Weboberfläche/für Agents, Adapter mit versch. Standards z. B. PKCS#7), PGP für On-Premise	ISO 27001/2 (Amazon AWS), SSL für Weboberfläche/Agenten, Adapter mit versch. Standards (z. B. OAuth2)“
b. Anwendungs- u. Plattformsicherheit	mandantenfähig, OWASP, lokale Laufzeit vorhanden	mandentenfähig, lokale Laufzeit vorhanden	mandentenfähig, lokale Laufzeit vorhanden	mandentenfähig, OWASP, lokale Laufzeit vorhanden	mandentenfähig, lokale Laufzeit nur via separaten MuleESB	mandentenfähig, gem HANA-Plattform (z. B. Tenant-Isolierung)	Mandentenfähig, lokale Laufzeit vorhanden
c. Datensicherheit	k. A. zur Datensicherung/-löschung von Metadaten	k. A. zur Datensicherung/-löschung von Metadaten	k. A. zur Datensicherung/-löschung von Metadaten	k. A. zur Datensicherung/-löschung von Metadaten	k. A. zur Datensicherung von Metadaten, Message Queues können ebenfalls gespeichert werden	k. A. zur Datensicherung/-löschung von Metadaten	k. A. zur Datensicherung/-löschung von Metadaten
d. Schlüsselmanagement	Verschlüsselung von Passwörtern, Schlüsselmanagement	k. A.	k. A.	Verschlüsselung von API-Passwörtern, k. A. zum Schlüsselmanagement	Verschlüssung von Passwörtern, k. A. zum Schlüsselmanagement	Schlüsselmanagement	Verschlüsselung von API-Passwörtern, Schlüsselmanagement
4.4 ID- u. Rechtemanagement	einfache Authent., rollenbas. Rechtemanagement	einfache Authent./LDAP, rollenbas. Rechtemanagement	einfache Authent., rollenbas. Rechtemanagement	einfache Authent., rollenbas. Rechtemanagement	einfache Authent./ externes ID-Mgmt (Oauth), rollenbas. Rechtemanagement	einfache Authent./Single Sign-On via Kerberos möglich, Policies, rollenbas. Rechtemanagement	einfache Authent, Single Sign-On via SAML-2/ LDAP möglich, rollenbas. Rechtemanagement
4.5 Kontrollmöglichkeiten für Nutzer	trust.boomi.com (rudimentär)	k. A.	trust.informaticacloud.com (rudimentär)	trust.jitterbit.com (rudimentär)	trust.mulesoft.com (rudimentär)	gem. HANA-Plattform	elastic.snaplogic.com/sl/dashboard.html
4.6 Monitoring u. Security Incident Management	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging	24/7 Monitoring/Incident-Mgmt, Logging
4.7 Notfallmanagement	k. A.	k. A.	k. A.	k. A.	k. A.	ISO 22301 (RZ)	k. A.
4.8 Portabilität u. Interoperabilität	rudimentärer Export von Mappings, Plattform API	im-/Export via CastIron Live Studio	Im-/Export via Power Center, Plattform API	Im-/Export via Jitterbit Studio	Im-/Export via Anypoint Studio, Plattform API	Im-/Export via Integration Designer u. Data Services	Im-/Export von Projekten, Platform API
4.9 Sicherheitsprüfung u. -nachweis	siehe 4.5	k. A.	siehe 4.5	siehe 4.5	siehe 4.5	gem. HANA-Plattform	siehe 4.5
4.10 Personalanforderungen	k. A.	k. A.	k. A.	definiert	k. A.	gem. HANA-Plattform	k. A.
4.11 Vertragsgestaltung							
a. Transparenz	rudimentär	rudimentär	rudimentär	umfassende Information	rudimentär	gem. HANA-Plattform	rudimentär
b. Service Level Agreements	k. A.	k. A.	k. A.	k. A.	k. A.	gem. HANA-Plattform	k. A.
4.12 Datenschutz u. Compliance	Sitz USA, Verarbeitung USA	Stammsitz USA, Verarbeitung in den USA /EU	Sitz USA, Verarbeitung USA /EU, SOC 1	Stammsitz USA, Verarbeitung in den USA /EU	Sitz USA, Verarbeitung USA /EU, SOC 1	Sitz EU, Verarbeitung USA/EU, 95/46/EG, SOC 1/3, ISO 9001	Verarbeitung in den USA (kein Safe-Harbor) oder EU
4.13 Integrität	keine zusätzl. Angaben	keine zusätzl. Angaben	keine zusätzl. Angaben	keine zusätzl. Angaben	keine zusätzl. Angaben	keine zusätzl. Angaben	keine zusätzl. Angaben

4.3.3 Datensicherheit

Die Plattformen verarbeiten zwar Integrationsdaten, speichern aber nur Metadaten. Detaillierte Angaben dazu, welchen Metadaten gespeichert werden, machen die Anbieter nicht. MuleSoft Cloudhub bietet optional Warteschlangen für Nachrichten an, die Integrationsdaten speichern. Detaillierte Angaben dazu, wie und wann die Daten gesichert werden, machen die Anbieter nicht. Bei der Nutzung der Infrastrukturen renommierter Anbieter wie Rackspace oder Amazon werden die Daten redundant gespeichert [Amazon (2014); Rackspace (2015)].

4.3.4 Schlüsselmanagement

Einzig SAP HCI erlaubt die Verschlüsselung der Daten auf der Plattform. Bei den anderen Anbietern beschränkt sich die Verschlüsselung auf die Anwendungspasswörter[6] (MuleSoft erlaubt zusätzlich die Verschlüsselung von Warteschlagen). Dell Boomi, SAP HCI und Snaplogic verwenden hierzu ein Public-Private-Key-Verfahren. Bei Dell Boomi wird bei der Erstellung eines Benutzerkontos ein Schlüsselpaar erzeugt und Anwendungspasswörter werden mit dem öffentlichen Schlüssel verschlüsselt. Allerdings wird das Schlüsselpaar einseitig beim Anbieter gespeichert, weswegen das Vorgehen letztlich nutzlos ist. Zur Laufzeit werden die Passwörter dann mit dem privaten Schlüssel entschlüsselt. IBM Cast Iron Live, Informatica Cloud, Jitterbit und Cloudhub machen keine Angaben dazu, wie Schlüssel verwaltet werden. Alle Anbieter machen keine Angaben zur Stärke der Verschlüsselung (z. B. RSA 2048 Bit).

4.4 ID- und Rechtemanagement

Alle Anbieter unterstützen standardmäßig nur die einfache Authentisierung mit Benutzername und Passwort. Eine Zwei-Faktor-Authentisierung wird von keinem Dienst angeboten. Allerdings unterstützen einige Anbieter z. B. die Authentisierung via Kerberos (SAP) oder die Einbindung eines externen Cloud-Dienstes zum ID-Management (z. B. OAuth-Protokoll via PingIdentity-Dienst). Alle Plattformen bieten ein rollenbasiertes Rechtemanagement, das z. B. regelt, welche Benutzer auf welche Integrationsprozesse zugreifen dürfen.

4.5 Kontrollmöglichkeiten für Nutzer

Die Anbieter machen keine Angaben dazu, welche Kontrollmöglichkeiten die Nutzer hinsichtlich des administrativen Zugriffs durch den Anbieter haben. Die Plattformen bieten rudimentäre Informationen zu Service-Parametern wie Verfügbarkeit (Ampelsysteme), Wartungsfenstern und Sicherheitsaktualisierungen an. Hierzu werden den Benutzern Statuswebsites bereitgestellt (z. B. trust.jitterbit.com). Die Parameter beziehen sich nur auf die Plattformen selbst, nicht jedoch auf die Internet-Verbindung zwischen Anbieter und Benutzer. Letztere ist nicht Gegenstand der Service-Level-Agreements der Anbieter und muss separat mit dem Internet-Service-Provider vereinbart werden.

4.6 Monitoring und Security-Incident-Management

Rund um die Uhr überwachen alle Anbieter die jeweilige Plattform und reagieren auf sicherheitskritische Vorfälle. Ebenfalls werden Anmeldungen und Änderungen von Benutzern und Administrationen protokolliert.

4.7 Notfallmanagement

Mit Ausnahme von SAP HCI, das über ein Notfallmanagement nach ISO 22301 verfügt, machen die Anbieter dazu keine Angaben.

[6] Informatica macht hierzu keine Angaben.

4.8 Portabilität und Interoperabilität

Die Plattformen nutzen häufig keine Webanwendungen sondern normale Windows/ Linux-Anwendungen (z. B. auf Basis von Eclipse) für den Entwurf der Integrationsprozesse. Diese können lokal gespeichert werden, befinden sich allerdings in proprietären Formaten. Bei Dell Boomi Atmosphere erfolgt auch der Entwurf im Web und ein Export der Integrationsprozesse aus der Plattform ist nicht möglich. Die einzige Ausnahme sind Datenabbildungen, die als einfache Excel-Dateien exportiert werden können. Einige Plattformen (z. B. Informatica Cloud, MuleSoft Cloudhub) bieten eine Plattform-API mit der alternativ zur Weboberfläche auf die Plattform zugegriffen werden kann.

4.9 Sicherheitsprüfung und -nachweis

Die Anbieter informieren Cloud-Nutzer in der Regel mittels der Statuswebsites (vgl. Kontrollmöglichkeiten für Nutzer) über sicherheitsrelevante Vorfälle und Penetrationstests.

4.10 Personalanforderungen

Lediglich Jitterbit macht Angaben zu Personalanforderungen [Jitterbit (2014)]. Allerdings umfassen auch die von manchen Anbietern umgesetzten Sicherheitsstandards bereits Sicherheitsanforderungen an das Personal (vgl. z. B. [ISO (2013)], Control A.7.2.2).

4.11 Vertragsgestaltung

4.11.1 Transparenz

Mit Ausnahme von Jitterbit und SAP HCI weisen die Anbieter nicht unmittelbar darauf hin, wo die Daten des Nutzers verarbeitet werden. Allerdings ergab die detailliertere Betrachtung, dass der Kunde zwischen verschiedenen Deployment-Lokationen für die Integrationsumgebung (Ausnahme: Dell Boomi) wählen kann (inkl. EU-Cloud). Ob dort oder an einem anderen Standort dann ebenfalls die Metadaten des Nutzers gespeichert werden, ist unklar. Subunternehmer werden nur rudimentär offengelegt (z. B. Amazon Web Services bei Jitterbit). Eingeschränkt informieren die Anbieter darüber, welche Informationen verarbeitet bzw. gespeichert werden.

4.11.2. Service-Level-Agreements (SLA)

Die Anbieter machen generell nur grundlegende Angaben zu SLA-Parametern („Boomi's goal is to achieve 99.99% Service Availability") und keine spezifischen sicherheitsrelevanten Angaben innerhalb der Service-Level-Agreements. Auch die Angaben zu Subunternehmern und deren Sicherheitsmaßnahmen sind rudimentär und beschränken sich meist nur auf deren Zertifizierungen („Amazon Web Services ist ISO 27001 zertifiziert").

4.12 Datenschutz und Compliance

Zum Zeitpunkt der Erstellung dieses Artikels ist unklar, wie die Anbieter mit Sitz in den USA auf die Außerkraftsetzung der „Safe-Harbor"-Liste reagieren. Drei US-Hersteller (Jitterbit, MuleSoft und Snaplogic) sind aber auch nicht auf der Liste aufgeführt, was aus europäischer Sicht kritisch einzustufen ist. Im Fall der Datenverarbeitung in der EU haben sich die Unternehmen an die EU-Datenschutzrichtlinie 95/46/EG zu halten (z. B. SAP weist auf deren Einhaltung explizit hin). Allerdings stellt sich auch hier die Frage, inwiefern US-Unternehmen Daten auf ihren EU-Servern an US-Behörden weitergeben. Von den betrachteten Unternehmen ist einzig SAP der Anbieter mit Stammsitz in der europäischen Jurisdiktion.

4.13 Integrität

Keiner der Anbieter macht hierzu weitergehende Angaben als die vorgenannten.

FAZIT

Die detaillierte Betrachtung der sieben ausgewählten Plattformen in Hinblick auf die Sicherheitsanforderungen des BSI ergab grundsätzlich, dass die öffentlich verfügbaren Informationen zu Informationssicherheit und Datenschutz der Anbieter unzureichend sind. Zwar werden technische Funktionalitäten im Detail beschrieben, Informationen zur Umsetzung der betrachteten Sicherheitsanforderungen sind insgesamt aber unvollständig. Folglich muss der Kunde einzeln im Dialog mit den Anbietern klären, inwiefern und wie Sicherheitsanforderungen erfüllt oder nicht erfüllt werden.

Aus unserer Betrachtung wurde z. B. nicht eindeutig ersichtlich, was der organisatorische und geographische Geltungsbereich der aufgeführten Zertifizierungen zum Sicherheitsmanagement-System überhaupt ist. Welche Daten effektiv beim Hersteller gespeichert werden und ob diese überhaupt verschlüsselt werden, geht ebenso aus den öffentlichen Angaben der Hersteller nicht hervor. Die meisten Anbieter verschlüsseln die kritischen Anwendungspasswörter der Anwendungsschnittstellen, machen aber keine Angaben zum Verfahren. Im Falle von Dell Boomi wird jedoch auf ein Publiy-Key-Konzept zur Verschlüsselung der Passwörter verwiesen, welches gänzlich unwirksam ist. Keiner der betrachten Anbieter nutzt beim Zugriff auf die Weboberfläche der Plattform eine starke Authentisierung (z. B. Zwei-Faktor-Authentisierung), wie diese beim E-Banking üblich ist. Welche Kontrollmöglichkeiten der Nutzer über die Prozesse des Anbieters hat, ist gleichsam intransparent und die über die Status-Websites bereitgestellten Informationen sind rudimentär.

Für den Fall, dass personenbezogene Daten verarbeitet werden sollen, ist zum jetzigen Zeitpunkt eindeutig von der Speicherung in der Cloud US-amerikanischer Anbieter abzuraten, weil unklar ist, welches Datenschutzniveau nach der Aussetzung der „Safe-Harbor"-Liste gewährleistet wird. Werden Dienste eines US-amerikanischen Anbieters genutzt, sollten die Daten allenfalls in einer lokalen Integrationsumgebung beim Kunden verarbeitet werden und es sollte überprüft werden, dass lediglich Metadaten in die Cloud übertragen werden. Als Alternative können die Dienste europäischer Unternehmen wie das dargestellte SAP HCI oder Elastic.io genutzt werden.

REFERENZEN

AICPA (2014): Service Organization Controls (SOC), http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx, zuletzt aufgerufen am 23. Juli 2015.

Amazon (2014): Amazon S3 – Produktdetails, https://aws.amazon.com/de/s3/faqs, zuletzt aufgerufen am 23. Juli 2015.

Boillat, T. und Legner, C. (2014): Why Do Companies Migrate Towards Cloud Enterprise Systems? A Post-Implementation Perspective, in: IEEE 16th Conference on Business Informatics, 1, 2014, S. 102-109. doi: 10.1109/CBI.2014.46.

BSI (2012): Bundesamt für Sicherheit in der Informationstechnik, Eckpunktepapier, Sicherheitsempfehlungen für Cloud Computing Anbieter, Bonn, 2012.

CSA (2014): Cloud Controls Matrix, https://cloudsecurityalliance.org/research/ccm/#_downloads, zuletzt aufgerufen am 21. Juli 2015.

Dell (2015): Data Communication Security, http://help.boomi.com/atomsphere/GUID-A5BD775D-E710-44D7-9322-98D3F3532DBC.html, zuletzt aufgerufen am 23. Juli 2015.

EU Kommission (2015): Model Contracts for the transfer of personal data to third countries, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm, zuletzt aufgerufen am 7. Oktober 2015.

EuGH (2015): PRESSEMITTEILUNG Nr. 117/15, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117de.pdf, zuletzt aufgerufen am 7. Oktober 2015.

Federrath, H. und Pfitzmann, A. (2000): Gliederung und Systematisierung von Schutzzielen in IT-Systemen, in: Datenschutz und Datensicherheit DuD, 24(12), 2000, S. 704-710.

Gola, P. und Schomerus, R. (2015): BDSG: Bundesdatenschutzgesetz – Kommentar, München, 2015.

ISO (2013): ISO/IEC 27001 – Information security management, International Organization for Standardization, 2013.

Jitterbit (2014): Jitterbit Harmony Security & Architecture Whitepaper, http://www.jitterbit.com/Files/Product/HarmonySecurityWhitepaper.pdf, zuletzt aufgerufen am 23. Juli 2015.

MuleSoft (2015): Virtual Private Network, https://developer.mulesoft.com/docs/display/current/Virtual+Private+Cloud, zuletzt aufgerufen am 23. Juli 2015.

OWASP (2013): OWASP Top 10 – 2013, https://www.owasp.org/images/4/42/OWASP_Top_10_2013_DE_Version_1_0.pdf, zuletzt aufgerufen am 23. Juli 2015.

Pezzini, M. und Lheureux, B. J. (2011): Integration platform as a service: moving integration to the cloud, in: Gartner, 2011, S. 1-9.

Pezzini, M., Natis, Y. V., Malinverno, P., et al (2015): Magic Quadrant for Enterprise Integration Platform as a Service, in: Gartner, 2015, S. 1-35.

Rackspace (2015): Cloud Block Storage: FAQs, http://www.rackspace.com/knowledge_center/product-faq/cloud-block-storage, zuletzt aufgerufen am 10. Oktober 2015.

Ring, K. (2000): EAI: Making the right Connections, in: Ovum Reports 1–9, Boston, 2000.

SAP (2013): SAP HANA Cloud Integration, https://help.sap.com/cloudintegration/SAP_HCI_Overview.pdf, zuletzt aufgerufen am 23. Juli 2015.

Tietz, V., Blichmann, G. und Hübsch, G. (2011): Cloud-Entwicklungsmethoden, in: Informatik-Spektrum, 34, 2011, S. 345-354. doi: 10.1007/s00287-011-0531-1

Vossen, G., Haselmann, T. und Hoeren, T. (2012): Cloud-Computing für Unternehmen: Technische, wirtschaftliche, rechtliche und organisatorische Aspekte, Heidelberg, 2012.