WHITE PAPER | DEZEMBER 2016

Auswahl der richtigen API-Management-Lösung für Anwender in Unternehmen

ca technologies

Die Chancen durch APIs

Die Anwendungsprogrammierschnittstelle (API) ist zwar ein altes Konzept; dieses wird jedoch zurzeit transformiert, da aufgrund der Anforderungen von Mobilität und Cloud mehr Unternehmen ihre Informationen für externe Entwickler offenlegen. Indem Unternehmen wie eBay, Expedia und Salesforce Daten über APIs für ihre Entwickler offenlegen, erzielen sie erfolgreich Umsätze an neuen Märkten. Laut ProgrammableWeb.com werden zurzeit über 16.000 offene APIs öffentlich über das Internet angeboten – während es 2005 erst 32 waren.[1]

Indem sie APIs für externe Entwickler offenlegen, gelingt es zahlreichen Technologie-Start-ups, zu Plattformen zu werden, da sie Entwicklercommunities fördern, die ihre wesentlichen Daten- oder Anwendungsressourcen nutzen. Dies bedeutet eine größere Reichweite (wie beispielsweise beim schnellen Wachstum von Twitter), höheren Umsatz (wie bei AppExchange von Salesforce.com) oder bessere End-User-Bindung (wie bei Facebook).

Nicht nur Technologie-Start-ups verwenden APIs, um Informationen und Funktionalität für externe Entwickler verfügbar zu machen. Initiativen zur Integration von Cloud, Mobilität und Partnern veranlassen weitere Unternehmen dazu, APIs zu verwenden, um ein Ökosystem von Entwicklern um sich herum aufzubauen und somit mehr Reichweite sowie Umsatz- und Kundenbindungsmöglichkeiten im Zusammenhang mit ihren Informationen zu erreichen. Anders als viele Start-ups müssen große Unternehmen sich dem Thema API-Veröffentlichung jedoch sehr vorsichtig nähern: Bei ihnen steht viel auf dem Spiel, einschließlich ihres guten Rufs, der Einhaltung von Vorschriften und des Gleichgewichts zwischen den Anforderungen von Kunden, Partnern, Mitarbeitern und Aktionären.

Die Herausforderung des API Management in Unternehmen

Die Veröffentlichung von APIs für eine externe Entwicklercommunity, seien es Partner oder die Öffentlichkeit, bedeutet eine Reihe von Herausforderungen und Risiken für das Unternehmen. Wie schützen Sie die Informationen, die Sie offenlegen, vor Missbrauch oder Angriffen? Wie stellen Sie Ihre APIs als zuverlässige Services ohne Ausfallzeiten für die Anwender bereit? Wie steuern Sie Zugriff und Nutzung Ihrer APIs konsistent mithilfe von Richtlinien? Wie verdienen Sie mit Ihren APIs Geld? Wie helfen Sie Entwicklern, Ihre APIs zu finden und ihren Zugriff darauf selbst zu verwalten? Diese Fragen sind sowohl für Start-ups als auch für große Unternehmen relevant; für die IT-Organisationen großer Unternehmen sind sie jedoch akuter und dringender. Unternehmen können es sich nicht leisten, dass eine übereilte API-Management-Strategie ihrem Ruf schadet, und vor allem müssen sie sorgfältig gestaltete IT-Prozesse und -Schutzmechanismen aufrechterhalten.

Unabhängig davon, was für eine Art von API ein Unternehmen offenlegen möchte, benötigt es eine API-Management-Lösung, die einige grundlegende Funktionsbereiche abdeckt:

- **API Security**: Unternehmen können es sich nicht leisten, dass ihre Informationen oder Anwendungsressourcen, die sie über eine API verfügbar machen, missbraucht werden.
- **API Life Cycle Management**: Unternehmen benötigen eine Möglichkeit, sicherzustellen, dass API-Updates keine Schäden verursachen, wenn sie Upgrades oder neue Versionen von APIs bereitstellen oder APIs zwischen Umgebungen, Standorten, Rechenzentren und der Cloud verschieben.
- **API Governance**: Unternehmen benötigen eine Möglichkeit, die umfassenderen betrieblichen Implikationen der Offenlegung von APIs für unterschiedliche Partner und Entwickler über Richtlinienmerkmale wie Messungen, SLAs, Verfügbarkeit und Performance zu steuern und zu verfolgen.
- **Flexibilität für die Bereitstellung**: API-Management-Lösungen sollten in die vorhandene Infrastruktur des Unternehmens integrierbar sein.
- **Unterstützung von Entwicklern und Aufbau einer Community**: Unternehmen benötigen eine Möglichkeit, Entwicklern ein Onboarding zu bieten, sie zu verwalten und ihnen zu helfen, die offengelegten APIs optimal zu nutzen.
- **Monetisierung von APIs**: Einigen Unternehmen genügt es nicht, ihre APIs nur zu veröffentlichen. APIs bedeuten auch neue Umsatzchancen, und unterschiedliche API-Management-Lösungen ermöglichen die Monetisierung in unterschiedlichem Ausmaß.

Für Unternehmen ist es unerlässlich, dass diese Funktionsanforderungen erfüllt werden. Zugleich erwartet ein Unternehmen jedoch auch, dass seine API-Management-Lösung bestimmte betriebliche Merkmale aufweist, die für seine einzigartige IT Experience relevant sind.

- **Security der Lösung**: Da API-Management-Lösungen in der „demilitarisierten Zone“ (DMZ) bereitgestellt werden, benötigen Unternehmen auch robuste API-Lösungen der IT-Klasse, die eine Reihe von Security-Anforderungen erfüllen können, vom Schutz vor Eindringlingen über die PCI-Einhaltung und FIPS bis hin zur HSM-Unterstützung für die Security mit API-Schlüsseln.
- **Verwaltbarkeit der Lösung**: Unternehmen verfügen über Entwicklungs-, Test- und Produktionsumgebungen, die mehrere geografische Standorte, Rechenzentren und Clouds umfassen. Daher benötigen sie eine API-Management-Lösung, die zu ihren spezifischen Entwicklungsstilen und -prozessen passt.
- **Zuverlässigkeit der Lösung**: Unternehmen, die APIs kommerziell veröffentlichen, erwarten eine Uptime von 99,999 %, wenn nicht höher, und können sich keine Ausfälle leisten. Was sind die Merkmale einer robusten und verfügbaren Lösung?

In diesem White Paper werden diese unterschiedlichen funktionsbezogenen und betrieblichen Anforderungen untersucht, um IT-Managern, Web-Managern und Unternehmensarchitekten wichtige Informationen für die Auswahl einer API-Management-Lösung an die Hand zu geben.

Funktionsanforderungen an eine API-Management-Lösung

API Security

Bei der Suche nach einer API-Management-Lösung sind Security-Funktionen häufig das, woran potenzielle Käufer zuerst denken – vor allem dann, wenn der Käufer ein Unternehmen ist, das unabhängig von Standards wie SOAP, REST oder JSON wichtige Informationen schützen möchte, die über eine API offengelegt werden. Die Sorgen um die API Security beginnen mit der Access Control. Für APIs, die für Externe zugänglich sind, bedeutet dies, dass Folgendes möglich sein muss:

- Akzeptieren unterschiedlicher Arten von Anmeldeinformationen für die Authentifizierung
- Ausgeben unterschiedlicher Arten von Anmeldeinformationen an Entwickler
- Unterstützen unterschiedlicher Ressourcenautorisierungsschemas, einschließlich Federation-basierter wie OAuth, OpenID Connect und SAML

Für Unternehmen wird diese Herausforderung noch verschärft, da sie Integrationen in ihre vorhandene Identitätsinfrastruktur durchführen müssen. Daher besteht das übergreifende Ziel darin, Flexibilität und Integration zu erreichen. Die Richtlinien sollten eine Möglichkeit bieten, unterschiedliche Arten von Zugriffstoken zu unterstützen und sogar von einer Art der API-Entwicklerschlüssel zu einer anderen zu wechseln, ohne Code schreiben oder verändern zu müssen. Die Lösung sollte in der Lage sein, zahlreiche unterschiedliche OAuth-Schemas zu unterstützen, da dies die Standards für die Mobile Security und für APIs sind. Die Lösung sollte jedoch auch unterschiedliche Arten von OAuth, wie HMAC (Hash Message Authentication Code) mit Schlüsseln, und Kombinationen mit Unternehmensstandards wie SAML (Security Assertion Markup Language) verarbeiten können. Natürlich muss die API-Management-Lösung auch mit bereits vorhandenen Investitionen in Identitätslösungen von Unternehmen wie CA Technologies, IBM, Oracle und RSA zusammenarbeiten.

API Security ist jedoch mehr als Access Control. APIs bieten das Fenster, durch das Programme auf Ihre Daten zugreifen können. Daher muss eine API-Management-Lösung der Enterprise-Klasse dem Unternehmensarchitekten oder dem Security-Administrator eine spezifische Kontrolle darüber ermöglichen, welche Daten offengelegt werden, wie diese Informationen vertraulich gehalten werden und wie ihre Übertragung gegen Abfangen oder Manipulation gesichert werden kann.

Außerdem beruht die API Security auf der Integrität der API ebenso wie auf der Integrität der Daten und Funktionen, die sie offenlegt. Daher muss sichergestellt werden können, dass APIs nicht durch Angriffe, Denial-of-Service-Attacken oder Missbrauch kompromittiert werden. Eine gute API-Management-Lösung bietet ihrem Betreiber zahlreiche Steuerungsmechanismen für den Schutz vor Bedrohungen, mit denen die Zuverlässigkeit und Präzision der API und der durch sie ermöglichten Kommunikation sichergestellt werden können.

API Life Cycle Management

APIs werden nicht in einem Vakuum erstellt. Wie jede Anwendungsfunktionalität benötigen APIs ihren eigenen Entwicklungslebenszyklus, vom Design über Programmierung und Testing bis zur Bereitstellung. Daher muss es möglich sein, Änderungen an einer API während dieses gesamten Entwicklungslebenszyklus zu verfolgen, unabhängig davon, ob beim Entwicklungsprozess das Wasserfallmodell oder ein agiler Ansatz verwendet wird. Daher benötigt jede API-Management-Lösung Workflows mit umfassender Funktionalität für folgende Aspekte:

- Planung und Design von APIs anhand von Branchenstandards
- End-to-End-Integration und -Security für APIs
- Testing, Bereitstellung und die Möglichkeit zu Versionssteuerung und Rollbacks
- Management und Monitoring der API-Nutzung, einschließlich Berichte und Analysen

Für eine API-Management-Lösung mit vollständiger Funktionalität sollte es auch möglich sein, mehrere Versionen gleichzeitig in der Produktion zu verwenden, entweder, um ältere Clients zu berücksichtigen, oder um unterschiedliche Zugriffstechnologien wie SOAP (Simple Object Access Protocol), REST (REpresentational State Transfer) und JSON (JavaScript® Object Notification) einzubeziehen. Ein Framework für das Life Cycle Management, das ausschließlich die Entwicklung lokaler Lösungen unterstützt, erfüllt nicht die Anforderungen der meisten heutigen Unternehmen. Öffentliche und private Clouds werden immer wichtiger. Daher benötigen Unternehmen eine API-Management-Lösung, die Testing und Produktion in der Cloud einbezieht, sowie die Möglichkeit, API-Entwickler von den Eigenheiten der Netzwerke und Topologien zu isolieren.

API Governance

Governance ist ein umfassender Begriff, der häufig verwendet wird, um zahlreiche unterschiedliche Anforderungen an Management, Prozesse und Transparenz zu erfassen. Er definiert die Nutzungsbedingungen, unter denen eine API für einen oder mehrere Nutzer offengelegt wird. Während die Governance Security- und Lebenszykluskonzepte umfasst, beschreibt sie auch unterschiedliche Anforderungen an SLAs, Überwachung und Reporting. Außerdem ist die Governance im Fall von API-Management-Lösungen relevant für die umfassendere Notwendigkeit, differenzierte Nutzungsbedingungen zu ermöglichen, wenn API-Daten und -Funktionalität für unterschiedliche Nutzer freigegeben werden; berücksichtigt werden sollten hierbei ihre Identitäten, Fähigkeiten, Abonnementlevels oder sonstigen Transaktionskontexte, die in Richtlinien definiert werden können.

Bei der effektiven API Governance geht es vor allem um Flexibilität. Die Technologie, mit der gesteuert wird, wie APIs gemeinsam genutzt werden, sollte sich den Präferenzen und Prozessen des Unternehmens anpassen – und nicht umgekehrt. Dies bedeutet, dass eine API-Management-Lösung auf der Grundlage jeder richtlinienbasierten Steuerungsmethode mit SLAs, Security, Protokollen oder sonstige Faktoren konfigurierbar sein sollte. Richtlinien bilden das Kernstück der Flexibilität und stellen die Konsistenz zwischen einer Implementierung und der nächsten sicher. API-Management-Lösungen, die Administratoren nur allgemein definierte Steuerungsmechanismen ohne eine IDE mit vollständigen Richtlinien bieten, grenzen ein, was gesteuert werden kann und wie.

Flexible Bereitstellung

Die vorhandene Infrastruktur der meisten Unternehmen ist passend zu ihren Geschäftsvorgängen entworfen. Wenn das Unternehmen sich nach einer API-Management-Lösung umsieht, sollte es Lösungen evaluieren, die in seine vorhandene Umgebung integriert werden können. Architekturteams sollten in der Lage sein, diese Lösung als eine Erweiterung ihrer Infrastruktur zu verwalten statt als eine separate Umgebung. Weitere Informationen zu diesem Integrationslevel finden Sie im Lösungsüberblick „Architekturhandbuch für die Erweiterung Ihrer ESB/SOA-Umgebung auf Mobilität, Cloud und IoT“.

Unterstützung von Entwicklern und Aufbau einer Community

Gute API Governance stellt sicher, dass der Veröffentlicher die API konsistent steuern kann. Wenn diese API jedoch nicht leicht von externen Entwicklern gefunden und genutzt werden kann, riskiert der Veröffentlicher, dass niemand sie verwendet. Daher umfassen die meisten heutigen API-Management-Lösungen mehr als Steuerungsfunktionen wie Security, Lebenszyklus und Governance und bieten auch Funktionalität, mit der Veröffentlicher Informationen zu ihren APIs für externe Entwickler verfügbar machen können – häufig über Entwicklerportale. Ein Entwicklerportal bietet einen einzelnen Interaktionsort, an dem sich der Entwickler für einen Account registrieren, einen API-Zugriffsschlüssel anfordern, die verfügbaren APIs finden und sich Beispielcode ansehen kann.

Ein API-Entwicklerportal für die Nutzung durch Unternehmen sollte Folgendes bieten:

- Bereitstellung leicht nutzbarer mobiler APIs (auch für OAuth und OpenID Connect)
- Bereitstellung von Reporting und Analysen für Operatoren
- Unterstützung eines mühelosen Geschäftsbeziehungsmanagements

Da unterschiedliche Unternehmen mit unterschiedlichen Erfahrungen und Prioritäten an die Veröffentlichung von APIs herangehen, wäre ein unflexibler Standardansatz für das API-Portal nicht attraktiver als ein unflexibles Standard-Framework für Security, Lebenszyklus und Governance von APIs. Daher sollten viele Unternehmen ein mehrteiliges API-Portal in Erwägung ziehen. Dies könnte ein neutrales Portal (White-Label-Portal) sein, das an die jeweilige Strategie für die Entwicklereinbindung angepasst werden kann. Es könnte auch ein API-Portal sein, das in Form separater Komponenten über ein bereits vorhandenes Entwicklerportal des Unternehmens genutzt werden kann. Auch hier ist Flexibilität das Stichwort.

API-Monetisierung

Das Konzept der Monetisierung steht im Zusammenhang mit dem Gedanken der Entwicklerunterstützung. Während viele Unternehmen die Verwendung fördern möchten, indem sie kostenlosen Zugriff auf ihre Web-APIs und mobilen APIs ermöglichen, möchten andere nutzungsbasierte Zahlungsoptionen für höhere Zugriffsstufen anbieten. Auch auf die Frage nach dem richtigen Ansatz für die Monetisierung gibt es keine einzelne richtige Antwort. Einige Optionen sind:

- Ein „Freemium"-Modell, bei dem die Verwendung unterhalb eines bestimmten Schwellenwerts für die Datenübertragung oder einer bestimmten Anzahl Clientanforderungen kostenlos ist
- Gebühren für eine bestimmte Service-Level-Garantie oder für Priorität gegenüber nicht zahlenden Anwendern
- Angebot von Premium-Informationen oder -Funktionalität, die nur zahlende Kunden bekommen

Unabhängig vom ausgewählten Ansatz sollte die API-Management-Lösung ausgereift genug sein, um dem Unternehmen eine flexible Gestaltung seiner Umsatzkriterien zu ermöglichen. Die Lösung sollte zu Folgendem in der Lage sein:

- Erfassung eines Spektrums von Nutzungsstatistiken als Grundlage für Verbrauchsmessungen
- Bereitstellung fortschrittlicher SLA- und Class-of-Service-Funktionen zur Zuordnung von Prioritäten zu Datenverkehr
- Zusammenstellung virtueller, nur für zahlende Kunden verfügbarer APIs mit Isolationsmöglichkeit, ohne zu programmieren

Betriebliche Anforderungen an eine API-Management-Lösung

Security der Lösung

Da eine API-Management-Lösung häufig das einzige technologische Element ist, das Unternehmens-APIs von der Außenwelt trennt, ist das Security-Level, das die Lösung für APIs bereitstellen kann, nur so stark wie die Security der Lösung selbst. Wenn die Lösung kompromittiert wird, ist die für die APIs gebotene Security gleichermaßen kompromittiert. Daher sollten Unternehmen, die API-Management-Lösungen untersuchen, die Security der Lösung als absolut wichtigen Gesichtspunkt ansehen.

Diese Lösungen sollen als Zwischenglied zwischen der Außenwelt und den internen APIs dienen. Daher wird bei einer Bewertung häufig als Erstes analysiert, ob die Lösung selbst kompromittiert werden kann. Dies hängt davon ab, welche Art von Penetration-Testing für die Lösung durchgeführt wurde, wie eingeschränkt der Zugriff auf die Lösung ist und ob sie wichtige Schwachstellenprüfungen bestanden hat. Berücksichtigt werden sollten nach STIG (Security Technical Implementation Guide) getestete Lösungen, die PCI DSS-Zertifizierung (Payment Card Industry Data Security Standard) bei Lösungen, die Kreditkarteninformationen weitergeben sollen, die Einhaltung von FIPS (Federal Information Processing Standard) sowie die Common Criteria-Zertifizierung für Lösungen, die höhere Security-Standards für Behörden erfüllen müssen.

Für die meisten praktischen Zwecke ziehen Unternehmen häufig API-Management-Lösungen in Betracht, die mithilfe eines Proxys zwischen externen Anforderungen und einer internen API vermitteln. Als Zwischenglieder bieten API-Gateways den Vorteil klarer, integrierter Steuerungspunkte und Isolierung. Dies vereinfacht die Security-Zertifizierung und -Verwaltung (genau wie bei Netzwerkfirewalls). Einige unterstützen auch Onboard-HSM (Hardware Security Module) für die Verschlüsselung von API-Schlüsseln. In vielen Szenarien stellen API-Schlüssel außerdem den Großteil der Authentifizierung als Verteidigung gegen Missbrauch dar. Daher ist es klug, diese Schlüssel durch Verschlüsselung vor Diebstahl zu schützen.

Verwaltbarkeit der Lösung

Anders als ein typisches Start-up, das seine gesamte Produktionswebseite beispielsweise über eine einzelne Amazon-Instanz oder einen kleinen Hosting Provider ausführt, verfügt ein großes Unternehmen im Allgemeinen über unterschiedliche Entwicklungs- und Produktionsumgebungen. Hierzu gehören:

- geografisch verteilte Entwicklerteams
- Produktionsumgebungen, die Rechenzentren weltweit einbeziehen
- Cloud-basierte Disaster-Recovery-Systeme

Daher steht die Verwaltbarkeit bei jeder Auswahlentscheidung im Mittelpunkt. Überlegungen etwa zum Management von Clustern von API Gateways, zur geografischen Lastverteilung, zum Betrieb in einer Lights-Out-Rechenzentrumsumgebung und zum Umgang mit Spitzenlasten sind wichtiger als andere Leistungsmerkmale. Auch hier gilt: Nicht alle API-Management-Lösungen sind für die spezifischen Anforderungen eines Unternehmens entworfen. Bevor ein bestimmter Weg eingeschlagen wird, sollte daher sorgfältig evaluiert werden, wie unterschiedliche Lösungen Cluster Management, Failover, Lasten-Bursting, Disaster Recovery und andere betriebliche Managementfaktoren unterstützen.

Zuverlässigkeit der Lösung

Sobald ein Unternehmen entscheidet, ein API-Veröffentlichungsprogramm durchzuführen, wird es effektiv zu einem Service Provider für seine API-Nutzer, die sich sehr bald auf das Unternehmen verlassen und kontinuierliche Uptime erwarten. Daher ist es unvermeidlich, dass das Unternehmen bei der Auswahl seiner API-Management-Lösung großen Wert auf die Zuverlässigkeit legt. Das Unternehmen sucht nach Lösungen, in die Redundanz integriert ist und bei denen das Risiko von Ausfallzeiten extrem klein ist oder ganz eliminiert wurde. Es empfiehlt sich, nur API-Management-Lösungen mit folgenden Möglichkeiten in Betracht zu ziehen:

- Bereitstellung on-premise, in der Cloud oder in einer hybriden Umgebung (API-Gateway on-premise, Entwicklerportal in der Cloud)
- Bereitstellung vollständiger Redundanz unabhängig vom Bereitstellungsmodell
- Integration in Ihre vorhandene Infrastruktur
- Erfüllen von Security-Vorschriften

Fazit

Da keine zwei Unternehmen jemals genau die gleichen Anforderungen oder Umgebungen haben, kann eine unflexible Standardlösung für das API Management niemals sinnvoll sein. Allen Unternehmen gemeinsam ist jedoch die Notwendigkeit, Exzellenz in Funktionen und Betrieb zu erreichen. Die meisten Unternehmen, die beabsichtigen, APIs extern zu veröffentlichen, wünschen daher eine flexible, richtliniengesteuerte API-Management-Lösung, die die strikten Produktionsvorgaben eines Service Providers erfüllt, dessen Services ununterbrochen, überall und mühelos verfügbar sein sollen. Funktional gesehen erfordert dies eine API-Management-Lösung, die eine Reihe unterschiedlicher Security-Voraussetzungen erfüllt, verbreitete Entwicklungslebenszyklen berücksichtigt, über Richtlinien gesteuert werden kann, das Entwickler-Onboarding ermöglicht, die Einbindung der Entwickler fördert und Monetisierungsoptionen unterstützt. Betrieblich gesehen sollte die API-Management-Lösung sicher, verwaltbar und zuverlässig sein.

Nutzen Sie unabhängige Studien zur Auswahl einer API-Management-Lösung

Mehrere führende Analysteninstitute untersuchen API-Management-Technologien und veröffentlichen Berichte, in denen sie Anbieter vergleichen, um Unternehmen die Auswahl der besten Lösungen für ihre digitalen Strategien zu erleichtern. Auch Websites mit IT-Rezensionen wie IT Central Station können eine hervorragende Informationsquelle für Anbietervergleiche und Kundenrezensionen darstellen.

Kostenlose Exemplare der Anbietervergleichsberichte von führenden Analysten sowie Kundenmeinungen zu CA API Management finden Sie unter: **ca.com/de/products/api-management/why-ca-api-management.html**.

Kontakt mit CA Technologies

Wir freuen uns auf Ihre Fragen, Kommentare und allgemeines Feedback.

Weitere Informationen finden Sie unter **ca.com/api**.

Kontaktieren Sie CA Technologies unter ca.com/de.

CA Technologies (NASDAQ: CA) entwickelt Software, die Unternehmen bei der Umstellung auf die Application Economy unterstützt. Software steht in allen Branchen und in allen Unternehmen im Mittelpunkt. Von der Planung über die Entwicklung bis hin zu Management und Security arbeitet CA Technologies weltweit mit Unternehmen zusammen, um die Art, wie wir leben, Transaktionen durchführen und kommunizieren, neu zu gestalten – ob mobil, in der privaten oder öffentlichen Cloud oder in verteilten Systemen oder Mainframe-Umgebungen. Weitere Informationen finden Sie unter **ca.com/de**.

1 ProgrammableWeb API Directory, Dez. 2016, www.programmableweb.com/apis/directory