„DAS MANAGEMENT DER API-INFRASTRUKTUR DER UNTERNEHMEN WIRD ZUNEHMEND INEFFIZIENT."

Sebastian Rohr über die Bedeutung von APIs

VON TEMEL KAHYAOGLU

In unserer zunehmend digitalen und vernetzten Welt sind Application Programming Interfaces (APIs) die Bausteine, mit denen sich innovative neue Geschäftsmodelle errichten lassen. Wir sprachen mit Sebastian Rohr, CTO der Apiida AG, über die Bedeutung von APIs und über den zentralen Aspekt der Sicherheit.

Herr Rohr, APIs haben in den vergangenen Jahren zunehmend an Bedeutung gewonnen. Woran liegt das und für welche Bereiche gilt das besonders?

Viele Unternehmen – allen voran die großen Cloud-Anbieter wie Amazon – haben vor etlichen Jahren die Neuausrichtung ihrer internen IT auf digitale Schnittstellen in Form von APIs gestartet. Der überragende Erfolg von Netflix, Amazon Prime oder auch dem CRM Cloud-Dienst Salesforce basiert auf dem Paradigma der Nutzung von APIs. Im Gegensatz zur komplizierten Integration von IT-Diensten in einer Eins-zu-Eins-Beziehung, ermöglicht die Bereitstellung von Informationen über APIs eine schneller anpassbare Variante. Statt ein Webinterface mit möglichst vielen Funktionen zu überfrachten, nutzt Salesforce die Möglichkeit, den Großteil seiner CRM-Funktionen über APIs abzudecken. Größere Kunden sind damit in der Lage, die für sie spezifischen und wichtigen Funktionen über eine selbst erstellte Oberfläche oder eine im eigenen Corporate Design erstellte Smartphone App anzubieten. Der Video-on-Demand-Anbieter Netflix muss nicht je eine eigene App für 20 TV-Anbieter mit jeweils vier Produktreihen erstellen und pflegen, sondern definiert eine regelmäßig aktualisierte und funktional erweiterte API, die sorgfältig dokumentiert wird. Es obliegt den TV-Anbietern, ob sie bestimmte Funktionalitäten auf ihrem TV offerieren oder diese den Premium-Modellen aus dem eigenen Hause vorbehalten. Ähnliches gilt für die Wachstumsbranche der Paketdienste. Ohne eine entsprechende App könnten viele der Mehrwertfunktionen gar nicht realisiert werden. Doch auch hier gilt: Wer den Aufwand der Pflege mehrerer Apps scheut, sollte besser in eine ordentlich spezifizierte, umgesetzte und dokumentierte API investieren und den Partnern im Netzwerk den gesicherten Zugriff ermöglichen. Nicht nur etablierte Unternehmen wie die Lufthansa oder der Beleuchtungsspezialist Osram setzen bereits auf die Digitalisierung ihrer Geschäftsprozesse und die Erschließung neuer Einkommensströme durch das Anbieten neuer APIs.

Wie müssen APIs ausgestaltet sein, um für Unternehmen den größtmöglichen Nutzen zu generieren?

Wie in vielen Bereichen der New Economy dominierten am Anfang eine hohe Dynamik und eine geringe Tiefe und Feinheit der Dokumentation die Landschaft der öffentlich verfügbaren APIs. Einige der frühen Anbieter solcher APIs sind heute bereits wieder vom Markt verschwunden, weil es an Strategie, Planung und Dokumentation der Abhängigkeiten fehlte. Nach neuesten Erkenntnissen grenzen sich erfolgreiche Unternehmen im Bereich der Digitalisierung gerade durch eine strategische Planung ihrer API-Landschaft und eine exzellente Dokumentation eben dieser APIs von den weniger erfolgreichen Unternehmen ab. Einen besonders großen Schritt nach vorne hat hierbei die Veröffentlichung der Open API Specification (OAS) gebracht. Aber heute sollte der Fokus ganz klar auf den Mehrwerten liegen, die eine Ausrichtung auf APIs dem Unternehmen bringen kann. Sehen Sie sich die Lufthansa an, die sich mit ihrer Open API-Initiative gegenüber Dritten öffnet und sich selbst und anderen damit neue Vertriebskanäle und Umsatzströme eröffnet. Oder blicken Sie auf Osram, die als ehemaliger Leuchtmittelhersteller nun Beleuchtungskonzepte für Events und Lokationen anbieten, die ganzheitlich über deren API-Plattform geplant, konfiguriert und betrieben werden können. Das sind ganz neue Geschäftsmodelle, die sich durch APIs erst sinnvoll und kosteneffizient umsetzen lassen!

Auf der anderen Seite sind diese APIs aber auch beliebte Angriffspunkte für die Cyberkriminalität – was macht sie so anfällig?

Schnell implementierte (weil schlecht geplante) APIs bieten auf sehr einfache Art Zugriff auf Informationen und Funktionen, die vormals hinter gut abgesicherten Anwendungsoberflächen mit starker Authentisierung versteckt waren. Die Sicherheit dieser alten Applikationen war zumeist durch ein ordentliches Konzept für das Identity and Access Management (IAM) definiert. Eine Vielzahl der heute veröffentlichten APIs unterliegt leider noch keiner solchen Reglementierung, und in den Unternehmen fehlen auch oft Vorgaben für den Schutz und die Absicherung der APIs gegen unerlaubte Benutzung. Dabei kann die Sicherheit der APIs mit ein wenig Planung und den richtigen Werkzeugen sehr einfach sein. Die Nutzung von API-Keys, Zertifikaten sowie die Definition der richtigen Zugriffsrechte schützen vor einem Großteil der in den Medien verbreiteten Angriffe. Im Grunde sollte das den API-Planer und schon gar nicht den Programmierer weiter tangieren: Mit einem solide vorbereiteten Developer-Portal und gutem API-Management werden die Sicherheitsmaßnahmen von Beginn an vordefiniert und sind auch nicht zu umgehen.

Worin bestehen die Herausforderungen im Management der API?

Das Management der komplexen API-Infrastruktur der Unternehmen wird, durch die diversen Sicherheitsanforderungen und die stetig steigende Anzahl zu verwaltender APIs, zunehmend ineffizient. Wir haben schon erlebt, wie Sicherheitseinstellungen für APIs zwischen den Gateways in Amerika und denen in Europa manuell über eine Exceltabelle abgeglichen wurden. Dass man hiermit keine agile Software-Entwicklung oder ein effizientes DevOps-Schema umsetzen kann, ist klar. Das Bestreben sollte sein, diese Ineffizienz und Unsicherheitsfaktoren bei der Verwaltung großer API-Landschaften durch sinnvolle Automation und umfassendes Monitoring kritischer Eigenschaften, wie zum Beispiel der Antwortzeiten, zu minimieren. Ganz am Ende muss jedoch der Anwender im Mittelpunkt stehen. Kein noch so interessanter Service wird vom Kunden akzeptiert, wenn die Usability miserabel ist. Das gilt insbesondere für Sicherheitsfunktionen wie die Anmeldung an einem System, einer App oder API.

Sie haben sich neben der Digitalisierung ebenso der Sicherheit verschrieben und bieten seit Kurzem auch eine innovative Lösung für die Authentifizierung von Mitarbeitern an. Erzählen Sie uns mehr über die Entwicklung und Funktionsweise des Produkts.

Bereits als Mitarbeiter der Siemens AG Ende der Neunzigerjahre wurde ich mit der Sicherheitstechnologie der Smartcards konfrontiert. Als Sicherheitsberater im Konzern war ich einer der ersten 100 Mitarbeiter, die einen multifunktionalen Dienstausweis zur Verfügung gestellt bekamen. Dieser kleine Tausendsassa der IT-Sicherheit ermöglichte es mir, sowohl mein Essen in der Kantine zu bezahlen, mir Snacks am Automaten zu kaufen, das Gebäude zu betreten und mich am eigenen Rechner anzumelden. Das Thema mit der sicheren E-Mail haben wir Profis einige Wochen zum Laufen zu bringen versucht, haben es dann aber aufgrund zu hoher Komplexität doch wieder gelassen. So schön und sicher die Smartcard als Mittel zur Anmeldung am PC auch scheint: Die fehlende Anwenderfreundlichkeit und die hohen Kosten sowie die Komplexität der Gesamtlösung haben der Smartcard nur wenige Freunde in den Konzernen verschafft. Außerdem habe ich meinen Ausweis immer wieder gerne zu Hause vergessen – und dann kam ich weder ins Büro noch konnte ich mich am PC anmelden. Vielleicht haben mich diese besonders unangenehmen Erfahrungen aus der Frühzeit meiner Karriere eingeholt, als wir unser Apiida Mobile Authentication (oder kurz AMA) entwickelt haben. Für mich als Sicherheitsexperte stand fest, dass Mitarbeiter eine starke Authentisierung im Konzernumfeld nur dann lieben lernen werden, wenn mit höchstem Anwenderkomfort und unter Verwendung bereits in den Tagesablauf integrierter Komponenten funktioniert. Den sogenannten „Millennials“ (also den gerade in die Unternehmen einströmenden jungen Mitarbeitern) ist das Smartphone ja geradezu an die Hand gewachsen, und auch viele Kollegen unserer Altersklasse und darüber hinaus legen den kleinen Handschmeichler selten beiseite. Die Wahrscheinlichkeit, dass ich mein Smartphone zu Hause vergesse, ist viel kleiner, als dass ich meinen Geldbeutel auf der Kommode liegenlasse. Wir haben uns an der Benutzerfreundlichkeit von Apple orientiert und eine möglichst sichere Authentisierung auf Basis der im Smartphone verbauten Sicherheitschips entwickelt. Ich bin davon überzeugt, dass diese Kombination aus Usability und Security viel mehr Freunde findet, als die Smartcard jemals hatte.

Komplexe Systemstrukturen und eine zunehmende Anzahl an Schnittstellen und Microservices erfordern eine zentrale Verwaltung und kontinuierliches Monitoring. Wie hilft der Apiida API Gateway dabei?

Unser Apiida API Gateway Manager überwacht in Echtzeit alle angeschlossenen API Gateways und Services. Wenn vordefinierte Grenzwerte (zum Beispiel die Antwortzeit von einem Backend) gerissen werden, werden die entsprechenden Verantwortlichen sofort benachrichtigt. Dadurch wird sichergestellt, dass ein Fehler so schnell wie möglich bemerkt wird und dadurch auch schneller behoben werden kann. Gleichzeitig unterstützt das Produkt die Verwaltung unterschiedlicher Versionen der APIs. Das Migrieren von neuen Versionen von der Entwicklung über das Testen und die Qualitätskontrolle bis hin zur Produktion kann aufwendig und fehlerhaft sein. Hier unterstützt API Gateway den IT-Betrieb und sichert den gesamten Prozess durch Automatismen ab, denn Flüchtigkeitsfehler können dem Menschen nun mal passieren.

Wie schätzen Sie die zukünftigen Entwicklungen ein und welche Pläne hat die Apiida, um auf diese Entwicklungen zu reagieren?

APIs und die Digitalisierung werden in deutschen Unternehmen mehr und mehr relevant. In den anderen Ländern, allen voran die USA, ist dieses Thema schon sehr viel weiter in den Unternehmen angekommen. Einen Vorsprung hat der, der mit Schnelligkeit und Innovation umzugehen weiß. Wir versuchen, mit innovativen Lösungen den Unternehmen einen möglichst einfachen Start in diese Thematik liefern zu können. Gleichzeitig haben wir uns Security auf die Fahnen geschrieben, um von Anfang an einen ganzheitlichen Sicherheitskontext liefern zu können.

SEBASTIAN ROHR

Sebastian Rohr ist seit 2016 Vorstand und CTO der Apiida AG. Das Thema Sicherheit prägt seinen gesamten Werdegang – so war er unter anderem Forscher für Netzwerksicherheit im Fraunhofer Institut für Sichere Informationstechnik.

Apiida AG
apiida.com
info@apiida.com